EXECUTIVE WARMAKING AUTHORITY AND OFFENSIVE CYBER OPERATIONS: CAN EXISTING LEGISLATION SUCCESSFULLY CONSTRAIN PRESIDENTIAL POWER?

Eric Lorber[*]

On March 19, 2011, the North Atlantic Treaty Organization ("NATO") launched strike aircraft and tomahawk cruise missiles against Libya in the opening phases of Operation Odyssey Dawn, the military intervention meant to stem Colonel Muammar Gaddafi's attacks on Libya's civilian population.[1] The purpose of these initial strikes was to destroy Libya's command and control facilities and its air defense network so that allied warplanes could fly uncontested through Libyan airspace and attack marauding government forces at will.[2] This strategy—seizing air superiority in the early stages of a military conflict and then proceeding to attack the enemy's ground forces and command systems—has been a hallmark of U.S. military operations in the post-Cold War era.[3]

Behind the scenes, however, the Obama administration and Pentagon officials considered heavily modifying this battle-tested approach with a

* J.D. Candidate, University of Pennsylvania Law School, Ph.D Candidate, Duke University Department of Political Science. I would like to thank Professor William Burke-White, Professor Matthew Waxman, Professor Ryan Goodman, Elan DiMaio, and Amara Levy-Moore for their helpful comments and keen editorial eyes. I would also like to thank the editorial staff of the *University of Pennsylvania Journal of Constitutional Law*. Any errors are my own.

1 *See* Liz Sly, Greg Jaffe, and Craig Whitlock, *U.S. and European officials say initial assault on Gaddafi's forces "very effective"; Libyan leader pledges "long, drawn-out war"*, WASH. POST (Mar. 21, 2011, 12:07 AM), http://www.washingtonpost.com/wp-dyn/content/article/2011/03/19/AR2011031903274_pf.html (detailing the initial reports of successful combat operations in Libya).

2 *See* Brad Knickerbocker, *U.S. leads "Odyssey Dawn" initial attack on Libya*, CHRISTIAN SCI. MONITOR (Mar. 19, 2011, 7:19 PM), ("In essence, [the] attacks were meant to shape the battle space so that coalition aircraft from other countries can safely enforce the no-fly zone.").

3 *See* MICHAEL R. GORDON & GENERAL BERNARD E. TRAINOR, THE GENERALS' WAR 205–23 (1995) (illustrating the tension among U.S. generals during the first hours of the Persian Gulf War when the United States launched a large attack against an impressive Iraqi air defense network using stealth aircraft); David A. Fulghum, *Fast Forward: The Pentagon's Force-Transformation Director Takes an Early Swipe at What Worked and What Didn't in Iraq*, AVIATION WK. & SPACE TECH., Apr. 2003, at 34–35 (describing the U.S. attack on Iraqi air defenses during Operation Iraqi Freedom that effectively disabled Iraq's ability to contest U.S. air superiority throughout the 2003 campaign).

radical, new addition: offensive cyberattacks.[4] In the lead-up to the March 19 attack, the administration debated disabling and destroying the Libyan air defense network and command and control nodes through concerted computer attacks that would prevent Libyan radars from effectively tracking allied aircraft.[5] During these discussions, the administration raised a number of questions without clear answers, most notably whether a cyberattack could trigger invocation of the requirements of the War Powers Resolution.[6] Although ultimately deciding to rely on more traditional kinetic operations, the administration's internal discussions highlight an emerging area of importance and uncertainty in both national security and the law: what domestic legal rules do and *should* govern the use of offensive cyber operations ("OCOs"), and how do these new capabilities play into the long-standing debate over the proper balance between congressional and executive war-making power?[7]

Yet a surprising amount of uncertainty exists as to which—if any—domestic laws constrain the use of OCOs and how they fit into the congressional-executive balance. As policymakers, scholars, and journalists have lamented, a coherent policy framework governing the use of OCOs does not exist and many questions remain unanswered.[8] Would an attack

---

4 *See* Eric Schmitt & Thom Shanker, *U.S. Weighed Use of Cyberattacks to Weaken Libya*, N.Y. TIMES, Oct. 18, 2011, at A1 (describing a debate within the Obama Administration as to the wisdom—and legality—of using cyberattacks in operations against Libya in 2011). For the purposes of this Comment, I define "cyberattacks" as "efforts to alter, disrupt, or destroy computer systems or networks or the information or programs on them . . . . [E]ncompassing activities that range in target (military versus civilian, public versus private), consequences (minor versus major, direct versus indirect), and duration (temporary versus long-term) . . . ." Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 422 (2011) (arguing that, for the foreseeable future, the United States will have to operate in an international legal environment that is unclear regarding whether cyberattacks constitute a use of force).

5 Schmitt & Shanker, *supra* note 4.

6 *See id.*; 50 U.S.C. §§ 1541–1548 (2006).

7 *See generally* JOHN HART ELY, WAR AND RESPONSIBILITY: CONSTITUTIONAL LESSONS OF VIETNAM AND ITS AFTERMATH (1993); LOUIS FISHER, PRESIDENTIAL WAR POWER (1995); MICHAEL J. GLENNON, CONSTITUTIONAL DIPLOMACY (1990); LOUIS HENKIN, CONSTITUTIONALISM, DEMOCRACY, AND FOREIGN AFFAIRS (1990); HAROLD HONGJU KOH, THE NATIONAL SECURITY CONSTITUTION: SHARING POWER AFTER THE IRAN-CONTRA AFFAIR (1990); FRANCIS D. WORMUTH & EDWIN B. FIRMAGE, TO CHAIN THE DOG OF WAR: THE WAR POWER OF CONGRESS IN HISTORY AND LAW (2d ed. 1989); Robert H. Bork, *Erosion of the President's Power in Foreign Affairs*, 68 WASH. U. L. Q. 693 (1990); Henry P. Monaghan, *Presidential War-Making*, 50 B.U. L. REV., Special Issue 1970, at 19; W. Michael Reisman, *Some Lessons from Iraq: International Law and Democratic Politics*, 16 YALE J. INT'L L. 203 (1991); Eugene V. Rostow, *"Once More Unto the Breach": The War Powers Resolution Revisited*, 21 VAL. U. L. REV. 1 (1986).

8 *See Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command: Before the S. Armed Services Comm.*, 111th Cong. 9 (Apr. 15, 2010), *available at* http://armed-services.senate.gov/statemnt/2010/04%20April/

using cyber weapons trigger the requirements of the War Powers Resolution?[9] Would OCOs be subject to reporting requirements under the Intelligence Authorization Act?[10] Conversely, do cyber operations grant the executive branch another tool with which it can prosecute attacks but avoid reporting and responding to congressional inquiries? These questions are largely unanswered both because the rise of OCOs is a relatively recent phenomenon and because much of the information about U.S. technical capability in this field is highly classified.[11]

Yet addressing these questions is increasingly important for two reasons. First, as states such as China, Israel, Russia, and the United States use these weapons now and likely will do so more in future conflicts, determining the domestic legal strictures governing their use would provide policymakers and military planners a better sense of how to operate in cyberspace.[12] Second, the possible employment of these tools adds yet another wrinkle to the battle between the executive and legislative branches over war-making authority.[13] In particular, if neither the War Powers Resolution nor the Intelligence Authorization Act governs OCOs, the executive may be allowed to employ U.S. military power in a manner largely unchecked by congressional authority.[14] As a result, the employment of these tools

---

Alexander%2004-15-10.pdf [hereinafter *Advance Questions*] ("President Obama's cybersecurity sixty-day study highlighted the mismatch between our technical capabilities to conduct operations and the governing laws and policies, and our civilian leadership is working hard to resolve the mismatch."); Ellen Nakashima, *Pentagon is debating cyber-attacks*, WASH. POST, Nov. 6, 2010, at A1 [hereinafter Nakashima, *Pentagon is debating cyber-attacks*] (discussing the so-far-unsuccessful attempts to establish a coherent legal framework governing offensive cyber operations).

9 *See* 50 U.S.C. § 1541a (2006) ("[T]he purpose [is] to . . . insure that the collective judgment of both the Congress and the President will apply to the introduction of United States Armed Forces into hostilities, or into situations where imminent involvement in hostilities is clearly indicated by the circumstances . . . .").

10 50 U.S.C. § 413b (2006) (regulating the use and reporting of covert action).

11 DEP'T OF DEF. CYBERSPACE POLICY REPORT: REPORT TO CONGRESS PURSUANT TO THE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2011, SECTION 934 (Nov. 2011), at 5 [hereinafter DEP'T OF DEF. CYBERSPACE POLICY REPORT] (responding to congressional inquiries as to how the Defense Department plans on using offensive cyber capabilities in future operations).

12 *See infra* Part I.

13 *See supra* note 7 and accompanying text.

14 For example, if, in the case of Operation Odyssey Dawn, the United States had decided to use cyberattacks to disable Libyan air defense systems, such an attack may not have triggered the reporting and removal requirements explicit in the War Powers Resolution. *See infra* Part IV. Though the Obama Administration argued that its military activities in Libya did not constitute hostilities for the purposes of the War Powers Resolution—and therefore did not trigger its reporting requirements—if U.S. forces were actively engaged in combat for a longer period of time such that the activities did constitute hostilities, determining whether cyberattacks trigger the War Powers clock would become critical in establishing when the executive was required to report and remove troops absent

implicates—and perhaps problematically shifts—the balance between the executive's commander-in-chief power[15] and Congress's war-making authority.[16]

This Comment provides an initial answer to the question of whether current U.S. law can effectively govern the Executive's use of OCOs.[17] It explores the interaction between this new tool and the current statutory limits on presidential war-making authority, with a particular focus on whether the two current federal laws meant to restrict executive power in this field—the War Powers Resolution[18] and the Intelligence Authorization Act[19]—apply to a wide range of potential offensive cyber operations undertaken by the executive branch. Beyond suggesting that neither the War Powers Resolution nor the Intelligence Authorization Act can effectively regulate most types of offensive cyber operations, this Comment suggests that while marginally problematic for a proper balance of war-making power between the executive and legislative branches, this lack of oversight does not fundamentally shift the current alignment. It does argue, however, that—given this lack of regulatory oversight—the President now has another powerful war-making tool to use at his discretion. Finally, the Comment suggests that this lack of limitation may be positive in some ways, as laying down clear legal markers *before* having a developed understanding of these capabilities may problematically limit their effective use.

This Comment proceeds by addressing these issues in five sections. Part I introduces the recent increase in offensive cyber operations and capabilities, both by the United States and other countries. It also discusses the underdeveloped nature of the law governing OCOs in the United States. Part II provides an overview of offensive cyber operations, specifically laying out a spectrum upon which different operations would fall (i.e., as stand-

---

congressional approval of the action. *Libya and War Powers: Hearing Before the Comm. on Foreign Relations*, 112th Cong. 14 (2011) (statement of Hon. Harold Koh, Legal Adviser, U.S. Dep't of State) [hereinafter *Libya War Powers*] ("[A] combination of four factors present in Libya suggests that the current situation does not constitute the kind of 'hostilities' envisioned by the War Powers Resolution's 60-day automatic pullout provision.").

15 U.S. CONST. art. II, § 2 ("The President shall be Commander-in-Chief of the Army and Navy of the United States . . . .").

16 U.S. CONST. art. I, § 8, cl. 11 ("Congress shall have power . . . To declare War, grant Letters of Marque and Reprisal, and make Rules concerning Captures on Land and Water . . . .").

17 This Comment explicitly does not address current U.S. legislative efforts to craft a framework that protects the private sector from foreign cyberattacks. *See, e.g.*, Cybersecurity Act of 2012, S. 2105, 112th Cong. (2012).

18 50 U.S.C. §§ 1541–1548 (2006) (restricting the deployment of U.S. soldiers in major combat operations for extended periods of time without the consent of either the President or Congress).

19 50 U.S.C. § 413b (2006).

alone operations or as a tactical supplement to major combat operations). Establishing this spectrum facilitates categorization of cyber operations and helps determine which domestic statutory framework would govern a particular type of operation.

Part III examines cyber operations through the prism of the War Powers Resolution, noting that while the Resolution is likely constitutional, an analysis of its language, Office of Legal Counsel ("OLC") opinions interpreting it, and case law suggests that it does not cover the use of offensive cyberattacks even if used as part of major military campaigns. Part IV examines whether the Intelligence Authorization Act provides Congress with regulatory power over stand-alone and covert operations, suggesting that, given its weak information-sharing requirements and substantially malleable language, the Act does not provide Congress with an effective regulatory mechanism. Part V discusses the implications of this lack of federal statutory coverage, in particular suggesting both that these new types of capabilities do not represent a substantial shift in the balance of war-making authority between the executive and the legislative branches and that, while critics lament the fact that it does not rein in presidential actions, the conclusion that it *should* is premature.

I. DEVELOPING OFFENSIVE CYBER CAPABILITIES, UNDER-DEVELOPING LEGAL FRAMEWORKS

Over the past five years, offensive cyber operations have become an increasingly frequent element of, inter alia, major combat operations,[20] coercive diplomacy,[21] and attempts to prevent nuclear proliferation.[22]

---

20 David Hollis, *Cyberwar Case Study: Georgia 2008*, SMALL WARS J., Jan. 6, 2011, http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008 (providing an in-depth assessment of how the Russians utilized cyberattacks *before* the start of kinetic operations to make those operations substantially more effective).

21 Ian Traynor, *Russia accused of unleashing cyberwar to disable Estonia*, GUARDIAN, May 17, 2007, http://www.guardian.co.uk/russia/article/0,,2081438,00.html. On coercive diplomacy more generally, see Robert J. Art, *Coercive Diplomacy: What Do We Know?*, *in* THE UNITED STATES AND COERCIVE DIPLOMACY (Robert J. Art & Patrick M. Cronin eds., 2003). The academic literature on coercion theory is vast and spans many decades. *See, e.g.*, RICHARD K. BETTS, NUCLEAR BLACKMAIL AND NUCLEAR BALANCE (1987); ALEXANDER L. GEORGE, FORCEFUL PERSUASION: COERCIVE DIPLOMACY AS AN ALTERNATIVE TO WAR (1991); ALEXANDER L. GEORGE & RICHARD SMOKE, DETERRENCE IN AMERICAN FOREIGN POLICY: THEORY AND PRACTICE (1974); THOMAS C. SCHELLING, THE STRATEGY OF CONFLICT (1980); THOMAS C. SCHELLING, ARMS AND INFLUENCE (1966); GLENN H. SNYDER & PAUL DIESING, CONFLICT AMONG NATIONS: BARGAINING, DECISION MAKING, AND SYSTEM STRUCTURE IN INTERNATIONAL CRISES (1977). For more recent works that have made an important contribution to the theory and the analysis of the empirical record, see DANIEL BYMAN & MATTHEW WAXMAN, THE DYNAMICS OF COERCION: AMERICAN FOREIGN POLICY AND THE LIMITS OF MILITARY MIGHT (2002); KENNETH A. SCHULTZ, DEMOCRACY AND COERCIVE DIPLOMACY (2001).

During this period, they have received a great deal of attention as newly effective methods of waging war, and indeed the United States, concerned both with developing defensive measures against enemies employing these capabilities, as well as determining how it will use its own offensive capabilities, has begun organizing around the notion that offensive cyber operations will constitute an important component of future warfare.[23] Yet during this time frame, despite the development and consideration of the employment of these capabilities, U.S. policymakers have been unable to effectively develop a legal framework for when they can and cannot be used.[24] The following discussion details some of the most notable public instances of the employment of offensive cyber operations over the past half-decade. It also describes how many policymakers and military strategists believe that cyber operations will become even more important in future combat operations. It then proceeds to discuss the comparatively underdeveloped legal rules and regulations governing the United States' use of such weapons.

A. Cyber Warfare Outside the U.S. Context

In what some journalists called the "world's first cyberwar," hackers linked to the Russian government attacked Estonian government websites and infrastructure in April and May of 2007.[25] In a series of attacks lasting approximately one month, Russian-linked hackers, responding to the removal of a Soviet statue in a port city, "came close to shutting down the country's digital infrastructure, clogging the Web sites of the president, the prime minister, Parliament and other government agencies, staggering

22 RICHARD A. CLARKE & ROBERT K. KNAKE, CYBERWAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 3–8 (2010) (suggesting that Israel took down Syrian air defenses with a cyberattack during its 2007 raid on Syria's nuclear reactor).

23 Siobhan Gorman & Yochi Dreazen, *Military Command Is Created for Cyber Security*, WALL ST. J., June 24, 2009, at A6 (detailing the establishment of Cyber Command to conduct offensive and defensive cyber operations); *see also* Donna Miles, *Gates Establishes New Cyber Subcommand*, AM. FORCES PRESS SERVICE (June 24, 2009), *available at* http://www.defenselink.mil/news/newsarticle.aspx?*id*=54890 (announcing the establishment of CYBERCOM).

24 Stewart Baker, *Denial of Service*, FOREIGNPOLICY.COM, Sept. 30, 2011, http://www.foreignpolicy.com/articles/2011/09/30/denial_of_service?page=0,0 (detailing the various, inchoate attempts to rein in cyber operations with outdated legal concepts).

25 Steven Lee Myers, *Estonia Computers Blitzed, Possibly by the Russians*, N.Y. TIMES, May 18, 2007, at A8 (providing an early assessment of how Russian-linked hackers—despite the Kremlin's denials—waged a cyber war against Estonia); Traynor, *supra* note 21; *see also* Jose Nazario, *Estonian DDoS Attacks—A summary to date*, ARBOR NETWORKS SEC. BLOG (May 17, 2007), http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/ (providing a detailed assessment of how Estonia's networks were taken down).

Estonia's biggest bank and overwhelming the sites of several daily newspapers."[26] The attackers used a network of "bots"—computers slaved to master servers and spread as widely as the United States and Vietnam—to overload Estonia's networks and shut down its ability to process information.[27] These Denial of Service ("DoS") and Distributed Denial of Service ("DDoS") attacks had a substantial effect on Estonia that went beyond making it impossible for Internet users to browse government websites; by attacking bank sites, the hackers were able to shut down online services and cause significant losses for financial firms.[28] Though Russia denied any link to the hackers, many in the cyber community—as well as in Estonia—believed the Russian government was responsible.[29] The incident raised two primary points of concern among national security officials and analysts around the world. First, though cyberattacks to steal information have been occurring for a long time (popularly dubbed "cyber exploitation"),[30] many thought this episode represented the first time a nation had employed a large-scale cyberattack to disable or destroy another country's infrastructure.[31] Second, compared to many other nations, experts considered Estonia to be particularly well prepared to deal with cyberattacks, as the government had teams and plans in place that actively confronted each intrusion throughout the episode.[32]

However, the Estonian attacks represented only one type of OCO undertaken in the past five years and likely the least damaging to the intended target.[33] In that case, though hackers were able to disrupt financial

---

26 Mark Landler & John Markoff, *After Computer Siege in Estonia, War Fears Turn to Cyberspace*, N.Y. TIMES, May 29, 2007, at 1 (detailing the initial attacks and providing a more substantial overview of the Russian-linked campaign); *see also* ENEKEN TIKK ET AL., INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS 14–35 (2010) (providing a comprehensive overview, including substantial background information, of the attacks on Estonia).

27 Landler & Markoff, *supra* note 26; John Robb, *When Bots Attack*, WIRED, Sept. 2007, at 166, 167 (laying out hypothetical scenarios for how China could launch a major bot attack against the United States and effectively disrupt the U.S. economy).

28 Landler & Markoff, *supra* note 26, at A1.

29 Jaak Aaviksoo, Minister of Def. of Est., Remarks at the Center for Strategic and International Studies: Cyberspace: A New Security Dimension at Our Fingertips (Nov. 28, 2007), *available at* http://csis.org/event/statesmens-forum-jaak-aaviksoo-minister-defense-republic-estonia (suggesting that Russia was responsible for the coordinated attack).

30 *See infra* notes 79–81 and accompanying text.

31 *See* Landler & Markoff, *supra* note 26.

32 *See* TIKK ET AL., *supra* note 26, at 24; Landler & Markoff, *supra* note 26; *Newly Nasty*, THE ECONOMIST, May 26, 2007, at 63 (suggesting that, following the mass-hacker attack against Estonia, most countries remained unprepared for this type of strike).

33 Interestingly, the damage of offensive cyber operations can spread far more broadly than their initial targets. *See* John Bumgarner & Scott Borg, U.S. Cyber Consequences Unit, *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008*, at 1 (2009), *available at* http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-

services and government websites, the long-term damage—to say nothing of the kinetic effects such as actual destruction—was limited.[34] Other countries have begun to use OCOs in more complex ways, particularly in conjunction with military operations. In 2008, during the Russian-Georgian war, the Russians—or Russian citizens operating with government approval—used denial of service attacks to disable government websites and prevent the Georgian authorities from providing information to the public.[35] In addition, the attacks made it more difficult for the government to transmit data to international observers and convince other countries of the magnitude of the Russian military assault.[36] The Russians also linked their OCOs with traditional kinetic operations for added effect; cyberattacks disrupted military communications between Georgian units and decreased the effectiveness of the Georgian defensive response.[37] According to military analyst David Hollis: "This appear[ed] to be the first case in history of a coordinated cyberspace domain attack synchronized with major combat actions in the other warfighting domains (consisting of Land, Air, Sea, and Space)."[38] Further, analysts believe that this tight linkage between kinetic

Cyber-Campaign-Overview.pdf (providing an in-depth examination of Russia's use of cyber operations against Georgia and suggesting that the 2008 Russian attack on Georgian servers had long-term echoes, with disruptions hitting Twitter and Facebook worldwide in 2009 as a direct result of the attack). This phenomenon of cyberattacks spreading more broadly than their intended targets is not limited to the Georgian case. *See* Robert McMillian, *Was Stuxnet Built to Attack Iran's Nuclear Program?*, PCWORLD (Sept. 21, 2010, 4:10 AM), http://www.pcworld.com/businesscenter/article/205827/was_stuxnet_built_to_attack_irans_nuclear_program.html (suggesting that though the Stuxnet worm may have been created to attack centrifuges at Iran's Natanz's nuclear energy facility, it damaged a wide range of industrial targets in India and Indonesia as well).

34 TIKK ET AL., *supra* note 26, at 24–25.

35 *Id.* at 77–79; *see also* Noah Shachtman, *Top Georgian Official: Moscow Cyber Attacked Us—We Just Can't Prove It*, WIRED (Mar. 11, 2009, 7:32 AM), http://www.wired.com/dangerroom/2009/03/georgia-blames/ (detailing how, despite invading the country, the Russian government denied that it employed its offensive cyber weaponry against Georgia). Others disagree with this portrayal. For example, the U.S. Cyber Consequences Unit suggested,

> The cyber attacks against Georgian targets were carried out by civilians with little or no direct involvement on the part of the Russian government or military. . . . The organizers of the cyber attacks had advance notice of Russian military intentions, and they were tipped off about the timing of the Russian military operations . . . .

Bumgarner & Borg, *supra* note 33, at 2–3.

36 TIKK ET AL., *supra* note 26, at 77–79.

37 Robert Haddick, *This Week at War: Lessons from Cyberwar I*, FOREIGNPOLICY.COM (Jan. 28, 2011), http://www.foreignpolicy.com/articles/2011/01/28/this_week_at_war_lessons_from_cyberwar_i (suggesting that Russia effectively coordinated its diplomatic, military, and cyber strategy to bring a great deal of coercive power to bear on Georgia); Hollis, *supra* note 20, at 2–5.

38 Hollis, *supra* note 20, at 2.

and cyber operations will become standard operating protocol in future military operations.[39]

In addition, the Israelis reportedly linked their cyber and kinetic operations—and plan to do so in the future—in conflicts against regional adversaries. In 2007, the Israelis launched Operation Orchard, a strike against a purported nuclear reactor being built in Syria with North Korean help.[40] Israeli aircraft penetrated Syrian airspace without detection or attack from Syria's air defense network.[41] Analysts believe that the Israelis were able to slip into Syrian airspace with non-stealthy aircraft due to a cyberattack—perhaps in the form of a kill switch that Israeli saboteurs placed inside electronics delivered to Syria—that disabled the air defense network.[42] Given the success of this operation, and particularly the fact that no Israeli aircraft were lost, many analysts believe that the Israelis will use a similar strategy if they decide to attack Iranian nuclear facilities.[43] The likelihood of future combatants deploying advanced cyberattacks alongside more traditional military forces is not limited to Israel and Russia. Notably, the Chinese have developed extensive OCOs designed to slow down deployments of U.S. troops into the Pacific theater in case of a U.S.-Chinese

---

39 *See, e.g.*, Ben Arnoldy, *Cyberspace: New Frontier in Conflicts*, CHRISTIAN SCI. MONITOR, Aug. 13, 2008, at 2 (arguing that Russia's use of offensive cyber operations portends the future integration of this capability into combat operations).

40 Mark Heinrich, *IAEA suspects Syrian nuclear activity at bombed site*, REUTERS (Feb. 18, 2010, 4:47 PM), http://www.reuters.com/article/2010/02/18/us-nuclear-syria-iaea-idUSTRE61H66320100218 ("[T]he International Atomic Energy Agency lent public support to Western suspicions that Israel's target was a nascent nuclear reactor that Washington said was North Korean in design and geared to making weapons-grade plutonium.").

41 *See* David A. Fulghum & Douglas Barrie, *Israel used electronic attack in air strike against Syrian mystery target*, ABC NEWS (Oct. 8, 2007), http://abcnews.go.com/Technology/story?*id*=3702807&page=1#.UJFmC47mWwo (exploring the electronic technology behind Israel's cyberattack which purportedly prevented advanced Syrian air defense systems from detecting inbound Israeli aircraft).

42 CLARKE & KNAKE, *supra* note 22, at 3–8; Sally Adee, *The Hunt for the Kill Switch*, IEEE SPECTRUM (May 2008), http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch/0 ("Among the many mysteries still surrounding that strike was the failure of a Syrian radar—supposedly state-of-the-art—to warn the Syrian military of the incoming assault. . . . [Many] speculated that the commercial off-the-shelf microprocessors in the Syrian radar might have been purposely fabricated with a hidden 'backdoor' inside.").

43 Eli Lake, *Israel's Secret Iran Attack Plan: Electronic Warfare*, DAILY BEAST (Nov. 16, 2011, 6:28 PM), http://www.thedailybeast.com/articles/2011/11/16/israel-s-secret-iran-attack-plan-electronic-warfare.html (detailing how Israel would use offensive cyber operations in future conflicts to attack not only Iran's air defense networks, but also its "electric grid, Internet, cellphone [sic] network, and emergency frequencies for firemen and police officers").

conflict and to reduce their effectiveness once deployed, principally by attacking U.S. communication nodes.[44]

B. The United States and Offensive Cyber Capabilities

While these countries have been developing offensive cyber capabilities, the United States arguably has "the world's most powerful and sophisticated offensive cyberattack capability."[45] According to the former chief technology officer of the Defense Intelligence Agency, "[w]e have U.S. warriors in cyberspace that are deployed overseas" and "live in adversary networks."[46] Indeed, the United States was responsible for one of the first cyberattacks, targeting the Soviet Union in 1982.[47] Over the past decade, the United States has begun to devote an increasing amount of attention to defending against offensive cyber operations while developing its own offensive capabilities.[48] In 2009, the United States set up Cyber Command ("CYBERCOM"), co-housed with the National Security Agency, to help secure U.S. systems from cyberattack.[49] While initially billed as a way to better streamline the United States' ability to defend itself against cyber operations, it quickly became apparent that a major mission of the new command was to develop and deploy offensive cyber weaponry across the globe. Indeed, General Keith Alexander, the chief of Cyber Command and the director of the National Security Agency, has expressed a desire to have

---

44 *See* Bryan Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, U.S.-CHINA ECON. & SEC. REVIEW COMM'N, at 23–24 (2009) (describing China's current doctrine and how it might be employed in a national conflict with the United States).

45 Jack Goldsmith, *Can we stop the cyber arms race?*, WASH. POST, Feb. 1, 2010, at A17.

46 *Id.*

47 *See* THOMAS C. REED, AT THE ABYSS: AN INSIDER'S HISTORY OF THE COLD WAR (2004) (detailing a cyberattack on Soviet gas refining capabilities in 1982 which had substantial blowback effects by infecting and damaging non-targets).

48 CLARKE & KNAKE, *supra* note 22.

49 Gorman & Dreazen, *supra* note 23, at A6 (detailing the establishment of CYBERCOM to conduct both offensive and defensive cyber operations); *see also* Miles, *supra* note 23 (announcing the establishment of CYBERCOM). Interestingly, CYBERCOM is tasked with defending military websites, whereas the Department of Homeland Security is tasked with defending civilian cyber infrastructure. As a result, the United States civilian infrastructure is less prepared than the military infrastructure to defend against cyberattacks. *See* Ellen Nakashima, *Pentagon is debating cyber-attacks*, WASH. POST, Nov. 6, 2010, at A7 ("[I]n testimony to Congress in September, [General Keith Alexander, head of Cyber Command] warned that Cyber Command could not currently defend the country against cyber-attack because it 'is not my mission to defend today the entire nation.' If an adversary attacked power grids, he added, a defensive effort would 'rely heavily on commercial industry.'").

"sufficient maneuvering room for his new command to mount what he has called 'the full spectrum of operations' in cyberspace."[50]

Since the creation of Cyber Command, U.S. offensive cyber capabilities have come into greater focus.[51] Through leaks of classified information, U.S. journalists have provided the public with a glimpse of a number of offensive cyber operations conducted over a years-long time frame. Most notably, in June 2012, New York Times reporter David Sanger revealed that the United States—collaborating with Israel—had launched an unprecedented, coordinated series of cyberattacks on Iran's nuclear program, code-named "Olympic Games."[52] Even after one of the core elements of Olympic Games, the Stuxnet virus, began affecting systems outside of Iran's nuclear industry, the United States continued launching similar assaults against Iran.[53] More recently, another computer program targeting Iran's nuclear industry, the Flame virus, also became public.[54] In contrast to Stuxnet, which attacked certain computer systems it infected, the United States and Israel jointly developed Flame to covertly steal key secrets about Iran's nuclear program after infecting Iranian systems.[55]

Despite these leaks of classified information, offensive cyber capabilities remain one of the U.S. government's most closely-guarded secrets. For example, in its recently released Strategy for Operating in Cyberspace, the Department of Defense did not mention its offensive capabilities.[56] Further, in response to congressional questions during the debates over the 2011

---

50 Nakashima, *supra* note 49, at A1 (suggesting that "[o]ffensive actions could include shutting down part of an opponent's computer network to preempt a cyber-attack against a U.S. target or changing a line of code in an adversary's computer to render malicious software harmless. They are operations that destroy, disrupt or degrade targeted computers or networks").

51 Ellen Nakashima, *Pentagon: Cyber offense part of U.S. strategy*, WASH. POST, Nov. 15, 2011, *available at* http://www.washingtonpost.com/pentagon-cyber-offense-part-of-us-strategy/2011/11/15/glQArEAIPN_story.html ("The Pentagon is prepared to launch cyberattacks in response to hostile actions that threaten the government, military or U.S. economy . . . .").

52 David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, at 1 [hereinafter Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*] (elaborating on how the United States and the Israelis co-developed a number of different viruses to both gather intelligence on—and disrupt—Iranian nuclear facilities).

53 *Id.*

54 Ellen Nakashima, Greg Miller, & Julie Tate, *U.S. and Israel created 'Flame'*, WASH. POST, June 20, 2012, at A1 ("The United States and Israel jointly developed a sophisticated computer virus nicknamed Flame that collected intelligence in preparation for cyber-sabotage aimed at slowing Iran's ability to develop a nuclear weapon, according to Western officials with knowledge of the effort.").

55 *Id.*

56 DEP'T OF DEF. STRATEGY FOR OPERATING IN CYBERSPACE (2011) (detailing how the U.S. government would develop robust defenses and partner with the private sector to assure integrity of its cyber systems).

National Defense Authorization Act, the Department of Defense did not directly address—at least in an unclassified forum—the extent of U.S. offensive cyber capabilities, nor the policies governing them.[57] However, it did reference that these capabilities exist: "[T]he Department has the capability to conduct offensive operations. . . . DoD will conduct offensive cyber operations in a manner consistent with the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict."[58]

These limited references to offensive cyber operations, including how existing legal principles may govern them, are becoming more frequent in public discussions, however. For example, in its Cyberspace Policy Report, the Department of Defense indirectly alluded to such capabilities by briefly touching on the application of the War Powers Resolution to cyberspace: "Cyber operations might not include the introduction of armed forces personnel into the area of hostilities. Cyber operations may, however, be a component of larger operations that could trigger notification and reporting in accordance with the War Powers Resolution."[59] Though not discussing specific U.S. policies or capabilities, such statements echo the idea—explored above in the Russian, Israeli, and Chinese cases—that the United States is actively planning to utilize cyber operations in future conflicts. And in one of the most transparent discussions of U.S. OCOs to date, General Alexander appeared before the Senate Armed Services Committee in 2010 and answered questions about CYBERCOM's mission, including its offensive activities.[60] In response to advance questions by senators, he noted that CYBERCOM would serve "as the focal point for deconfliction of DOD offensive cyberspace operations."[61] More recently, in the 2012 House Conference Report for the National Defense Authorization Act, Congress specifically recognized U.S. offensive cyber capabilities:

> Congress affirms that the Department of Defense has the capability, and upon direction by the President may conduct offensive operations in cyberspace to defend our Nation, Allies and interests, subject to (1) the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict; and (2) the War Powers Resolution. . . .[62]

---

57 DEP'T OF DEF. CYBERSPACE POLICY REPORT, *supra* note 11, at 2–9.

58 *Id.* at 5.

59 *Id.* at 9.

60 *Advance Questions*, *supra* note 8 (suggesting that the United States is developing, and will deploy, greater offensive cyber capabilities in the future).

61 *Id.* at 1.

62 H.R. REP. NO. 112-329, at 255–56 (2011) (Conf. Rep.). *See also id.* at 686 ("[T]here is a lack of historical precedent for what constitutes traditional military activities in relation to cyber operations and [] it is necessary to affirm that such operations may be conducted

Further, as discussed, in the recent Libyan intervention, the Obama administration has actively considered using its offensive cyber capabilities in conjunction with kinetic operations.[63] The instances above suggest that many countries—the United States among them—are developing and deploying offensive cyber capabilities both as tools of deterrence and for war-fighting purposes. Further, these comments and documents suggest that in the United States, policymakers are beginning to grapple with how these new technologies may fall under current legal regimes and potentially alter the war-making balance between Congress and the President.

C. The United States, Offensive Cyber Capabilities, and Legal Gaps

While a large body of scholarship speaks to the question of whether—and how—international law governs the use of cyber weapons, few scholars have addressed the issue of whether U.S. domestic law provides guidance as to when and how these tools can be employed and whether Congress currently has the ability to effectively regulate their use. Since the late 1990s, scholars and practitioners have grappled with a number of issues related to whether cyberattacks constitute armed attacks, justify self-defense, or create national obligations to assist other countries under cyberattack.[64] In particular, international law scholars have considered whether offensive cyberattacks constitute the use of armed force under the UN Charter.[65] They have suggested that such conclusions should be determined by the damage inflicted.[66] Other scholars have looked to past instances of actions short of the use of kinetic force, such as economic sanctions, to argue that cyberattacks likely constitute acts of aggression.[67] Likewise, academics,

---

pursuant to the same policy, principles, and legal regimes that pertain to kinetic capabilities.").

63 Schmitt & Shanker, *supra* note 4.

64 DEP'T OF DEF., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS (May 1999), at 8–10, *available at* http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf (arguing that cyberattacks may not constitute armed attacks under international law); Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 885 (1999) ("This Article explores the acceptability under the *jus ad bellum* . . . [c]oncluding that traditional applications of the use of force prohibition fail to adequately safeguard shared community values threatened by [computer network attacks].").

65 *See, e.g.*, Daniel B. Silver, *Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter*, 76 INT'L L. STUD. 73 (2002).

66 *See* David E. Graham, *Cyber Threats and the Laws of War*, 4 J. NAT'L SECURITY L. & POL'Y 87 (2010) (concluding that the question of whether cyberattacks are considered "armed attacks" in international law should be answered with an eye as to their negative effects).

67 *See, e.g.*, Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U. J. INT'L L. AND POL. 57 (2001) (suggesting that economic sanctions are not as

examining similar questions, have asserted either that international law cannot—as currently understood—effectively deal with these issues, or that, for the foreseeable future, such questions will not be clarified.[68] Others have explored when cyberattacks can justify legitimate acts of self-defense.[69] Beyond the academy, policymakers have also actively discussed whether and how international law governs the use of offensive cyber operations.[70]

While many in the public sphere have paid a great deal of attention to the legality of offensive cyber operations, far less attention has been devoted to how domestic law interacts with the United States' employment of these capabilities. Indeed, policymakers have repeatedly noted "the mismatch between our technical capabilities to conduct operations and the governing laws and policies."[71] Over the past few years, studies have suggested that the United States has not developed such a legal framework and that whether current U.S. law—such as the War Powers Resolution—can regulate OCOs remains under-analyzed.[72] While some argue that attempting to develop such a framework will severely hamper the United States' ability to effectively conduct offensive cyber operations in future conflicts,[73] most analysts agree that "[t]oday's policy and legal framework for guiding and regulating the U.S. use of cyberattack is ill-formed, undeveloped, and highly uncertain."[74] To this point, most of the debate as to the legality of these operations has remained behind government doors.[75] Indeed, until very recently, scholars

---

damaging as cyberattacks and merely represent a cessation of trade with a target country, not an active attack on that country's infrastructure).

68 Duncan Hollis, *New Tools, New Rules: International Law and Information Operations*, (Temple Univ. Legal Studies Research Paper No. 2007-15), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1009224 (asserting that the current system of international law as applied to information operations such as cyberattacks "suffers from several, near-fatal conditions"); Waxman, *supra* note 4.

69 Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 208–09 (2002) (suggesting that offensive cyber operations constitute a use of force).

70 NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 241–82 (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009) (providing a wide-ranging overview of how different elements of international law might apply to cyberattacks).

71 *Advance Questions*, *supra* note 8, at 9.

72 *See* NAT'L RESEARCH COUNCIL, *supra* note 70, at 233 ("This report does not seek to resolve this controversy [as to whether the War Powers Resolution governs offensive cyber operations], but observes that notions of cyberconflict and cyberattack will inevitably cause more confusion and result in less clarity.").

73 *See* Stewart Baker, *Denial of Service*, FOREIGNPOLICY.COM (Sept. 30, 2011), http://www.foreignpolicy.com/articles/2011/09/30/denial_of_service?page=0,0 (detailing the various, inchoate attempts to rein in cyber operations with outdated legal concepts).

74 NAT'L RESEARCH COUNCIL, *supra* note 70, at 4.

75 *See* Nakashima, *Pentagon is debating cyber-attacks*, *supra* note 8, at A1.

have not paid substantial attention to these issues. To date, only a few articles,[76] blog postings,[77] and a National Resource Council report[78] have delved into this issue in any detail.

This lack of attention creates a series of problems in determining whether and how to regulate these operations. Most notably, before even addressing whether a new framework should be developed, the question arises as to whether the current domestic legal framework *can* govern the employment of these capabilities. Although many policymakers have suggested the current framework cannot govern OCOs, this question remains to be closely examined and argued. Only if the existing framework is found inadequate should legal scholars and practitioners design a new legal framework. Indeed, if, as Matthew Waxman argues, "strategy is a . . . driver of legal evolution,"[79] then new legal mechanisms may be required to ensure proper limitations on the executive's war-making abilities.

Though a full accounting of the potential domestic legal mechanisms governing the use of offensive cyber weapons is beyond the scope of this Comment, a first step in determining whether the current legal framework can be effective, at least partially, in governing the uses of these new weapons is to examine whether an appropriate procedural system exists as to regulate when and how they are employed. Though not delving into specifics about the use of these weapons, an operative, procedural framework that allows other governmental branches to review, understand, and potentially check the uses of these weapons provides an initial move towards their effective regulation. Though it may not be sufficient to fully clarify when and how the use of offensive cyber weapons may be legal, such a system at least would allow for oversight and hold the promise of helping policymakers better understand the conditions under which they can lawfully use these tools.

---

76 *See, e.g.*, Robert Chesney, *Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate*, 5 J. NAT'L SECURITY L. & POL'Y 539 (2012) (discussing how Congress, through the Intelligence Authorization Act, may be able to rein in the executive's use of cyber capabilities); Stephen Dycus, *Congress's Role in Cyber Warfare*, 4 J. NAT'L SECURITY L. & POL'Y 155 (2010) (describing the lack of sufficient federal laws governing cyber operations, particularly in the relationship between the legislative and executive).

77 Jack Goldsmith, *Quick Thoughts on the USG's Refusal to Use Cyberattacks in Libya*, LAWFARE (Oct. 18, 2011, 7:48 AM), http://www.lawfareblog.com/2011/10/quick-thoughts-on-the-aborted-u-s-cyberattacks-on-libya/ (discussing why the Obama Administration decided not to use cyber warfare at the commencement of the Libya campaign); Julian Ku, *Do Cyberattacks Fall Under the War Powers Act?*, OPINIO JURIS (Oct. 18, 2011, 8:15 PM), http://opiniojuris.org/2011/10/18/do-cyberattacks-fall-under-the-war-powers-act/ (raising the question in relation to the Libya case but not answering it).

78 NAT'L RESEARCH COUNCIL, *supra* note 70.

79 Waxman, *supra* note 4, at 425.

To this end, this Comment examines the two primary statutory tools through which Congress has tried to regulate executive military action: the War Powers Resolution and the Intelligence Authorization Act. There are two reasons to focus on these statutes. First, they apply to instances in which offensive cyber weapons will most likely be employed outside of surveillance and espionage actions: covert actions to disable and disrupt adversary systems and capabilities, and overt actions taken in conjunction with kinetic operations to degrade an adversary's ability to effectively conduct combat operations. Second, they are the primary means through which Congress has attempted to constrain the President's exercise of his constitutional Commander-in-Chief function.[80] Historically, and particularly since 1970, Congress has been reluctant to use its primary power, the power of the purse, to defund military activities, utilizing it only a handful of times.[81] As recent controversies over funding for wars in Iraq and Afghanistan, as well as the intervention in Libya illustrate, threatening to defund ongoing military operations is politically delicate and many legislators prefer to avoid taking such action.[82] Before proceeding to analyze OCOs through the prism of these two statutes, however, sharpening our understanding of the different types of OCOs is necessary.

II. TYPOLOGIES, EMPLOYMENT, AND OFFENSIVE CYBER OPERATIONS

Cyberattacks are "efforts to alter, disrupt, or destroy computer systems or networks or the information or programs on them . . . [,] encompassing activities that range in target (military versus civilian, public versus private), consequences (minor versus major, direct versus indirect), and duration (temporary versus long-term)."[83] While this definition provides broad

---

80 U.S. CONST. art. II, § 2 ("The President shall be Commander-in-Chief of the Army and Navy of the United States . . . .").

81 RICHARD F. GRIMMETT, CONG. RESEARCH SERV., RS20775, CONGRESSIONAL USE OF FUNDING CUTOFFS SINCE 1970 INVOLVING U.S. MILITARY FORCES AND OVERSEAS DEPLOYMENTS (2001) [hereinafter GRIMMETT, CONGRESSIONAL USE OF FUNDING CUTOFFS SINCE 1970] (detailing congressional actions to cut off funding under the Constitution for U.S. troops abroad).

82 *See* Matthew Yglesias, *Lack of Congressional Authorization for Use of Force is an Abdication of Responsibility, Not a Power Grab*, THINKPROGRESS.ORG (Mar. 20, 2011, 6:30 PM), http://thinkprogress.org/yglesias/2011/03/20/200278/lack-of-congressional-authorization-for-use-of-force-is-an-abdication-of-responsibility-not-a-power-grab/ ("Even if you completely leave the declaration of war business aside, congress' [sic] control over the purse strings still gives a determined congressional majority ample latitude to restrain presidential foreign policy. The main reason congress [sic] tends, in practice, not to use this authority is that *congress* [sic] *rarely wants to*.").

83 Waxman, *supra* note 4, at 422. For an alternate, though similar, definition, see Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. NAT'L SEC. L. & POL'Y 63, 63 (2010) ("'[C]yber attack' refers to the use of deliberate actions and operations—perhaps over an

guidance as to what may constitute a cyberattack, for the purposes of applying existing legal structures, the definition must be conceptualized in a way that usefully fits into those preexisting regimes. Because of the complexity and great number of potential means of cyberattack, this Comment groups such attacks based on *employment*, i.e., the way in which they are utilized and their intended purposes. Such an approach provides greater clarity as to which U.S. domestic legal regime will likely govern their employment. The following section proceeds by first discussing some of the technical details of cyberattacks and then moves into understanding how they have been—and likely will be—employed in future conflicts.

Before moving to a discussion of what cyberattacks are, it is important to note what they are *not*. They are not cyberexploitation, that is, "the use of actions and operations . . . to obtain information that would otherwise be kept confidential . . . . Cyberexploitations are usually clandestine and conducted with the smallest possible intervention that still allows extraction of the information sought."[84] The core difference between attack and exploitation is in the cyber operation's purpose; cyberattacks are meant to be destructive whereas cyberexploitation acquires information nondestructively.[85] While the term offensive cyber operations usually encompasses both attack and exploitative elements, here "OCO" refers only to attacks.[86]

At the most basic level, a cyberattack requires three elements: vulnerability; access; and payload.[87] A vulnerability is "an aspect of the system that can be used by the attacker to compromise" an adversary's network.[88] Given the increase in the number of complex systems employed by countries in the past two decades, many cyber defense analysts and computer experts agree that it is increasingly difficult to foresee and prevent vulnerability exploitation before attacks.[89] Access refers to the ability to deliver the payload into the target system such that it exploits the vulnerability. In particular, access to a target depends on whether the attack can be launched via remote access (e.g., by hacking into a computer network via the internet)[90] or close access (e.g., attacking a system through

---

extended period of time—to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and (or) programs resident in or transiting these systems or networks.").

84 Lin, *supra* note 83, at 63.

85 *Id.* at 63–64.

86 *Id.* at 64.

87 *See* NAT'L RESEARCH COUNCIL, *supra* note 70, at 83 (giving a technical account of the technology and operational considerations underpinning contemporary cyber-weapons).

88 *Id.*

89 *Id.* at 84.

90 *Id.* at 87.

the "local installation of hardware" via covert operatives).[91] The payload describes "the things that can be done once a vulnerability has been exploited. For example, once a software agent (such as a virus) has entered a given computer, it can be programmed to do many things—reproducing and retransmitting itself, destroying files on the system, or altering files."[92] Cyberattacks generally target a system's integrity (i.e., the system's ability to operate normally),[93] ability to discern proper authenticity (i.e., the system's ability to determine whether it should accept incoming data),[94] or its availability (i.e., whether users can properly access the system).[95] The resulting effects can be wide-ranging, including destroying data on networks, generating bogus network traffic, covertly altering data on the network, and degrading or denying service on the network.[96]

Depending on whether the systems being attacked are remote or close access, a number of assault avenues exist. In an attack on a remote access system, botnets are one of the prominent means of assault.[97] In a botnet attack, which usually aims to deny users access to the system (such as a government website in a denial of service or distributed denial of service attack), bots install themselves on internet-connected computers and then, responding to commands from a master computer, attack the target by overloading it with numerous requests for information, such as e-mails, sometimes numbering in the millions.[98] Because the target cannot sufficiently process the information, it becomes inoperative.[99] Other ways to attack remote access systems include worms and viruses, which are generally used to install "trojan horse" systems on many computers that will render those computers inoperable.[100]

Attacking close access systems may generally be more difficult given their lower degree of accessibility. However, one attack approach involves inserting malicious software into the supply chain of a system that will eventually become close access.[101] Such a strategy allows a compromised

---

91 *Id.*

92 *Id.* at 88.

93 *Id.* at 111.

94 *Id.*

95 *Id.* at 112.

96 Lin, *supra* note 83, at 69–70.

97 Scott Berinato, *Attack of the Bots*, WIRED, Nov. 2006, *available at* http://www.wired.com/wired/archive/14.11/botnet.html (detailing how bots conduct distributed denial of service attacks).

98 Robb, *supra* note 27.

99 For a more in-depth discussion of a bot-net attack, see NAT'L RESEARCH COUNCIL, *supra* note 70, at 92–96.

100 *Id.* at 97.

101 DEF. SCI. BD. TASK FORCE, U.S. DEP'T OF DEF., REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON MISSION IMPACT OF FOREIGN INFLUENCE ON DOD SOFTWARE 22 (2007),

machine or piece of software to enter into the close access system and then to be activated at a later point based on a variety of triggering mechanisms. Other attack routes include inserting compromised universal serial buses ("USBs") into close systems. Such an approach can be accomplished either by willing or unwilling insiders.[102]

Hypothetically, scholars and practitioners have postulated a number of ways in which states might use cyberattacks in future combat scenarios, depending on a wide range of factors.[103] This process of categorization is not novel, as U.S. military planners have attempted to produce useful typologies since the mid-1990s.[104] While many potential categorization schemas exist, and many involve different types of adversaries, vulnerabilities, technologies underpinning the attacks, etc., most seem to focus on a primary element: the relationship of the cyberattack to other operations. In particular, the schemas differentiate based on whether the attack is part of a larger, kinetic offensive, or simply an attack launched independently of such operations. For example, Gregory Rattray and Jason Healey, in their recent work, suggest multiple ways in which a state could launch such an attack, but underpinning each is a discussion of whether the attack is part of a larger military operation or conducted independently.[105]

---

available at http://www.acq.osd.mil/dsb/reports/ADA486949.pdf ("Net-Centric systems surely will attract sophisticated adversaries who can subvert the supply chain to replace or alter software or hardware, recruiting well-placed insiders and exploiting single-string dependencies.").

102 Steve Stasiukonis, *Social Engineering, the USB Way*, DARK READING (June 7, 2006, 4:15 AM), http://www.darkreading.com/security/news/208803634/social-engineering-the-usc-way.html (detailing a social engineering experiment where a cyber expert scattered compromised USB drives throughout a parking lot, believing that bank employees would use them in the bank's close system and consequently give him access. Over 75% of the USBs placed in the parking lot were inserted into the bank's computers).

103 Gregory Rattray & Jason Healey, *Categorizing and Understanding Offensive Cyber Capabilities and Their Use*, *in* NAT'L RESEARCH COUNCIL, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 77, 81–83 (2010) (suggesting that different types of cyberoperations be broken down based on a wide range of factors including: nature of adversaries, nature of targets, target physicality, integration with kinetic operations, scope of the effect, intended duration, openness, context, campaign use, initiation responsibility, and rational, initial timing, and initiation attack); *see also* Mike McConnell, *Cyber Insecurities: The 21st Century Threatscape*, *in* 2 AMERICA'S CYBER FUTURE: SECURITY AND PROSPERITY IN THE INFORMATION AGE 25 (Kristin M. Lord & Travis Sharp eds., 2011) (detailing how different types of adversaries—including non-state actors—would use different methods of cyberattack for different results).

104 U.S. Air Force, *Cornerstones of Information Warfare* (1997), *available at* http://www.iwar.org.uk/iwar/resources/usaf/iw/corner.html (describing an early attempt to classify different types of information warfare).

105 Rattray & Healey, *supra* note 103, at 84–91 (describing how cyberattacks could be utilized, inter alia, as a surprise assault on military targets (with kinetic attacks following), in

Likewise, William Owens, Kenneth Dam, and Herbert Lin differentiate between types of cyberattacks that directly support or are in conjunction with military operations,[106] and those conducted independently as covert action.[107]

Further, the distinction between cyberattacks launched independently as opposed to part of a larger operation properly characterizes most known cyber operations to date. On the one hand, states have launched a number of attacks in recent years independent of kinetic operations.[108] For example, the actions in Estonia in 2007—though potentially linked to the Russian government—were independent of any larger military assault.[109] More notably, the Stuxnet virus, which inflicted tremendous damage on the Iranian nuclear energy program by destroying its centrifuge cascades and much of its Uranium enrichment capability, was launched independent of military action.[110] Though no nation has taken responsibility for the virus, most analysts suggest that Israel, with the United States' help, designed and deployed the virus to hinder Iran's nuclear development.[111] On the other hand, because cyberattacks may make kinetic operations more effective, states have recently employed the two in conjunction.[112] For example, the alleged Israeli attack on Syria in 2007[113]—as well as the alleged Russian attack on Georgia in 2008[114]—both employed cyberattacks in conjunction with larger operations. In addition, U.S. war planning for Libya also included a cyber component, but only as part of a larger intervention.[115]

---

operational support for traditional, kinetic military operations, in support of special operations missions, or as stand-alone covert action).

106 NAT'L RESEARCH COUNCIL, *supra* note 70, at 177–82.

107 *Id.* at 193–98.

108 *Id.*

109 *See supra* text accompanying notes 25–32.

110 Michael Joseph Gross, *A Declaration of Cyber-War*, VANITY FAIR, Apr. 2011, http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104 (detailing, as substantially as possible without access to TS-SCI information, the employment of the Stuxnet virus against Iranian Uranium enrichment facilities); *see also* Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, *supra* note 52; David E. Sanger, *Iran Fights Malware Attacking Computers*, N.Y. TIMES, Sept. 26, 2010, at A4 [hereinafter Sanger, *Iran Fights Malware Attacking Computers*] (detailing Iran's continued fight to purge the worm from its centrifuge control systems); William J. Broad, John Markoff, & David E. Sanger, *Israel Test Called Crucial In Iran Nuclear Setback*, N.Y. TIMES, Jan. 16, 2011, at A1 (examining Israel's preparations when deploying the worm, in particular, establishing a mock set up of Iranian nuclear facilities).

111 Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, *supra* note 52; Broad, Markoff, & Sanger, *supra* note 110.

112 MARTIN C. LIBICKI, CYBERDETERRENCE AND CYBERWAR 146–47 (2009) (detailing how cyber operation disruption can be effective in conjunction with military operations).

113 *See supra* text accompanying notes 40–43.

114 *See supra* text accompanying notes 35–39.

115 *Supra* text accompanying note 14.

Given the historical record of cyberattacks and that most of the theoretical literature categorizes such attacks based on their relationship to military actions, this Comment divides the attacks into binary categories: attacks waged independently of other military operations, and attacks waged as part of a larger military campaign. Though such a distinction may blur as states employ their capabilities in innovative ways, relying on that distinction now will aid both in understanding how different U.S. domestic laws apply to both general categories and in better preparing legal analysts in case of future cyber operations that do not neatly fit into them. Given this distinction, the analysis below examines whether current U.S. law effectively governs offensive cyber operations performed in conjunction with a military campaign or as a stand-alone operation.

III. THE WAR POWERS RESOLUTION: ARMED FORCES, HOSTILITIES, AND STATUTORY INTERPRETATION

Before proceeding to a discussion of either the War Powers Resolution or the Intelligence Authorization Act, one must acknowledge the inherent tension built into the relationship between Congress and the President over the power to wage war. Notably, the Constitution splits war-making authorities between the congressional and executive branches.[116] Proponents of executive power suggest that, because the President is the "Commander in Chief of the Army and Navy of the United States,"[117] he is vested with the war-making power to determine when and how to deploy U.S. armed forces.[118] Conversely, Congress has the ability to "declare war," "raise and support Armies," "provide and maintain a Navy," and "provide for calling forth" and organizing and arming the militia.[119] Further, based on the Necessary and Proper Clause, some argue that Congress is empowered to pass legislation in accordance with its constitutional war-making authority specified above.[120] The debate over the extent of each branch's war-making

116 Stephen L. Carter, *The Constitutionality of the War Powers Resolution*, 70 VA. L. REV. 101, 101 (1984) ("Anyone wishing to argue that the War Powers Resolution of 1973 is unconstitutional must be prepared to explain the purpose of article I, section 8, clause 11, of the Constitution. That provision expressly grants to Congress the power 'To declare War.'").

117 U.S. CONST. art. II, § 2, cl. 1.

118 ANN VAN WYNEN THOMAS & A.J. THOMAS, JR., THE WAR-MAKING POWERS OF THE PRESIDENT 7–8 (1982).

119 U.S. CONST. art. I, § 8, cls. 11–16.

120 Patrick D. Robbins, Comment, *The War Powers Resolution After Fifteen Years: A Reassessment*, 38 AM. U. L. REV. 141, 148 (1988) (discussing the different constitutional bases of the Congress's war-making authority).

power has shadowed many conflicts in which the United States has been involved.[121]

The intensity of this debate increased considerably during the Vietnam War, when Congress, uncomfortable with Presidents Johnson and Nixon's continuation of the conflict, attempted to rein in presidential power through a series of legislative acts.[122] The ineffectiveness of these early actions led a Senate committee to propose the War Powers Act in 1972.[123] After a period of extensive debates in which the language of the original Act was modified,[124] the House of Representatives concurred with the Senate bill and passed the Resolution on October 12, 1973.[125] On November 7, the House of Representatives overrode President Nixon's veto[126] of the War Powers Resolution.[127]

Congress intended the War Powers Resolution ("WPR")[128]—passed in response to the Vietnam War when Presidents Kennedy, Johnson, and Nixon deployed large numbers of U.S. troops to Southeast Asia without a congressional declaration of war—to limit the President's power to send U.S. forces into combat without explicit congressional authorization.[129] However, given inherent questions about its constitutionality,[130] congressional unwillingness to invoke the authority granted to it under the

---

121 *Id.* at 150 ("Whatever the Framers' intent, Presidents in both the nineteenth and twentieth centuries consistently have tested the limits of their authority to make war.").

122 Michael Ratner & David Cole, *The Force of Law: Judicial Enforcement of the War Powers Resolution*, 17 LOY. L.A. L. REV. 715, 736 (1984) (exploring the conflict between the executive and legislative branches during the Vietnam war); *see generally* William B. Spong, Jr., *Can Balance be Restored in the Constitutional War Powers of the President and Congress?*, 6 U. RICH. L. REV. 1 (1971) [hereinafter Spong Jr., *Can Balance be Restored?*] (reviewing war power proposals by Congress prior to 1972).

123 S. 2956, 92d Cong., 2d Sess. (1972).

124 For an in-depth discussion of this process, see generally William B. Spong Jr., *The War Powers Resolution Revisited: Historic Accomplishment or Surrender?*, 16 WM. & MARY L. REV. 823, 823 (1975) [hereinafter Spong Jr., *The War Powers Resolution Revisited*] ("Reflecting unquestionably the divisiveness caused by the nation's long involvement in Southeast Asia, this legislative activity, which culminated in the enactment of the War Powers Resolution of 1973 . . . .").

125 119 CONG. REC. 33,858–33,873 (1973).

126 H.R. DOC. NO. 93-171 (1973).

127 119 CONG. REC. 36,201–36,222 (1973) (284-135 vote to override).

128 War Powers Resolution, Pub. L. No. 93-148, 87 Stat. 555 (1973) (codified at 50 U.S.C. §§ 1541–1548 (2006)) ("It is the purpose of this joint resolution to fulfill the intent of the framers of the Constitution of the United States and insure that the collective judgment of both the Congress and the President will apply to the introduction of United States Armed Forces into hostilities . . . .").

129 *See* Spong Jr., *The War Powers Resolution Revisited: Historic Accomplishment or Surrender?*, *supra* note 124, at 824–35; *see also* Ratner & Cole, *supra* note 122, at 728–29.

130 Carter, *supra* note 116, at 101–02 (debating the constitutional issues undermining the War Powers Resolution).

WPR under most circumstances,[131] and the likelihood that deploying offensive cyber activities does not constitute the introduction of armed forces into hostilities (if the hostilities threshold is even met),[132] the War Powers Resolution is a weak footing upon which to base congressional oversight of these activities.

The following section provides an overview of the provisions of the War Powers Resolution, paying particular attention to its reporting and withdrawal requirements. It then proceeds to discuss the debates over the Resolution's effectiveness and constitutionality, noting that while it has proven ineffective at times, it may not be fatally flawed or unconstitutional. Following, this section discusses the definitions of key terms, based both on how they have been interpreted in past historical instances of the Resolution's invocation and in the legislative history of the Act. Finally, this section argues that its terms likely do not cover offensive cyber operations launched independently or in conjunction with kinetic operations.

A. A Brief Overview of the War Powers Resolution

In the absence of congressional declaration of war, the WPR requires that:

> [T]he President shall submit within 48 hours to the Speaker of the House of Representatives and to the President pro tempore of the Senate a report, in writing, setting forth—(A) the circumstances necessitating the introduction of United States Armed Forces; (B) the constitutional and legislative authority under which such introduction took place; and (C) the estimated scope and duration of the hostilities or involvement.[133]

Three circumstances trigger this reporting requirement. If United States armed forces are introduced: (1) "into hostilities or into situations where imminent involvement in hostilities is clearly indicated by the circumstances;"[134] (2) if such forces are introduced "into the territory, airspace, or waters of a foreign nation, while equipped for combat, except for deployments which relate solely to supply, replacement, repair, or training of such forces;"[135] and (3) "in numbers which substantially enlarge United States Armed Forces equipped for combat already located in a

---

131 *See generally* John Hart Ely, *Suppose Congress Wanted a War Powers Act That Worked*, 88 COLUM. L. REV. 1379 (1988) (suggesting how Congress could amend the Resolution to make it more effective); *see also* RICHARD F. GRIMMETT, CONG. RESEARCH SERV., RL33532, WAR POWERS RESOLUTION: PRESIDENTIAL COMPLIANCE (2011) [hereinafter GRIMMETT, WAR POWERS RESOLUTION: PRESIDENTIAL COMPLIANCE].

132 *Libya War Powers*, *supra* note 14, at 7–9.

133 50 U.S.C. § 1543 (2006).

134 *Id.*

135 *Id.*

foreign nation."[136] Beyond requiring the President to submit a report to Congress within forty-eight hours of these specific triggering events, the WPR also directs the President to withdraw armed forces within sixty days after the report is submitted or is required to be submitted, unless Congress has declared war, extended the sixty-day period by law, or is physically unable to meet because of an armed attack against the United States.[137] The President can unilaterally extend this period for an additional thirty days.[138] In another controversial provision of the Act, Congress, by concurrent resolution, can order the President to remove U.S. armed forces if they are engaged in hostilities outside of the United States without a declaration of war or statutory authorization.[139] As discussed below, the constitutionality of this section (as well as the mandatory sixty-day removal requirement) is debatable, as the Supreme Court has ruled that legislative vetoes invalidating executive actions—which these sections arguably constitute—are unconstitutional.[140]

As becomes evident, based on the text of the Resolution, determining the definitions of "U.S. armed forces," "hostilities," "imminent," and "into the territory . . . while equipped for combat," is crucial for concluding whether the President must report U.S. military activities and remove U.S. forces after sixty days. Before analyzing whether such definitions might encompass offensive cyber operations, it is helpful to understand the primary arguments against the Act, including the routine assertion by Presidents that it is unconstitutional.[141]

B. The Alleged Weaknesses of the War Powers Resolution

Critics of the War Powers Resolution assert two broad critiques: that it is ineffective in practice and that it is unconstitutional.[142] Regarding the first

---

136 *Id.*

137 50 U.S.C. § 1544 (2006).

138 *Id.*

139 *Id.*

140 Immigration and Naturalization Serv. v. Chadha, 462 U.S. 919 (1983) (holding that legislative vetoes are unconstitutional). *See also* Process Gas Consumers Group v. Consumer Energy Council of Am., 463 U.S. 1216 (1983) (asserting that the ruling in *Chadha* is meant to be a broad rule and not limited to that case's particular facts). *But see* Hollingsworth v. Virginia, 3 U.S. 378 (1798) (holding that concurrent resolutions do not require approval by the President).

141 GRIMMETT, WAR POWERS RESOLUTION: PRESIDENTIAL COMPLIANCE, *supra* note 131, at 2 ("[E]very President has taken the position that it is an unconstitutional infringement by the Congress on the President's authority as Commander in Chief.").

142 For a list of other critiques, see Rostow, *supra* note 7, at 1–2 (detailing arguments suggesting that adherence to the War Powers Resolution would wreck the constitutional balance of power and would "restore the Articles of Confederation as our norm for

claim, analysts suggest that Presidents simply order operations that successfully evade WPR reporting and withdrawal requirements, despite the fact that U.S. soldiers are deployed in situations likely imagined by the statute's drafters.[143] In particular, administrations continually argue that situations into which U.S. troops are deployed do not constitute hostilities.[144] Likewise, some suggest that macro-scale operations of the kind triggering the War Powers Resolution—where lengthy troop deployments are followed by crises and subsequent war—are antiquated and unlikely to occur in contemporary times.[145] Other analysts simply claim that Presidents have ignored the reporting requirements[146] and that members of Congress have been unwilling to stand up to potentially popular presidential uses of force, even if they clearly violate the WPR.[147] As a result, some analysts believe that other congressional mechanisms, such as its funding powers, provide the body with stronger oversight ability over executive action.[148] While many have critiqued the War Powers Resolution for its apparent ineffectiveness, this does not necessarily suggest it is has been futile; Presidents have actively submitted reports pursuant to its requirements and therefore have at least provided Congress with information about their activities.[149]

---

handling the foreign affairs of the nation, and leave the United States drifting helplessly in stormy seas, naked before its enemies").

143 Robbins, *supra* note 120, at 160–73 (suggesting that the President has undertaken limited and covert operations, in part, because these can avoid triggering the "hostilities" element of the War Powers Resolution). *See also* Michael Mandel, Note, *A License to Kill: America's Balance of War Powers and the Flaws of the War Powers Resolution*, 7 CARDOZO PUB. L., POL'Y & ETHICS J., 785, 794–805 (2009) (detailing how the War Powers Resolution has been applied to limited- and large-scale troop deployments).

144 *Libya War Powers*, *supra* note 14, at 7–8; *see also* Michael J. Glennon, *The Cost of "Empty Words": A Comment on the Justice Department's Libya Opinion*, HARV. NAT'L SECURITY. J. (Apr. 14, 2011, 8:54 AM), http://harvardnsj.org/2011/04/the-cost-of-empty-words-a-comment-on-the-justice-departments-libya-opinion/ (critiquing the Obama Administration's view of its War Powers duties during the Libya campaign, particularly focusing on the weakness of the applicable statutes).

145 Michael J. Glennon, *Too Far Apart: Repeal the War Powers Resolution*, 50 U. MIAMI L. REV. 17, 20 (1995) (suggesting that, in its current form, the War Powers Resolution is ineffective). The proposition that such large operations are antiquated is dubious, however, as the United States deployed large numbers of troops to Kuwait and Saudi Arabia, and after a few months launched a military attack against Iraq.

146 *Id.* at 19. Through 2009, Presidents have submitted one hundred and twenty-seven reports pursuant to the War Powers Resolution. However, only one of these cited the 4(a)(1) section of the Act, which triggers the sixty-day time limit. RICHARD GRIMMETT, CONG. RESEARCH SERV., R41199, THE WAR POWERS RESOLUTION: AFTER THIRTY-SIX YEARS 49–69 (2010) [hereinafter GRIMMETT, THE WAR POWERS RESOLUTION].

147 *Id.*; *see also* Ely, *supra* note 131, at 1384 ("[T]he President has refused to obey the law, and Congress has not had the fortitude to call him on it.").

148 GRIMMETT, CONGRESSIONAL USE OF FUNDING CUTOFFS SINCE 1970, *supra* note 81, at 1.

149 GRIMMETT, THE WAR POWERS RESOLUTION, *supra* note 146, at 49–69.

In addition to critiquing its effectiveness, administrations and legal analysts have suggested that the WPR is unconstitutional or suffers from substantial legal problems.[150] These claims break down into four different assertions: that the War Powers Resolution infringes on the President's commander-in-chief function, based on an original understanding of these provisions by the Framers;[151] that the concurrent resolution constitutes a legislative veto of an executive action and is therefore unconstitutional under *Immigration and Naturalization Services v. Chadha*;[152] that members of Congress do not have standing to bring claims for presidential violations of the WPR;[153] and that enforcement of the WPR presents a non-justiciable claim.[154]

While each of these claims has merit, none is sufficiently definitive as to whether the Resolution is constitutional or suffers from other fatal legal flaws. First, good evidence exists to support arguments that the Framers would have found the Resolution to be consistent with congressional war powers,[155] or conversely, that it infringes upon the Executive's commander-in-chief function.[156]

Second, the War Powers Resolution may not constitute a "legislative veto" for the purposes of *Chadha*.[157] According to legal scholars, "[t]he

---

150 *See generally* Carter, *supra* note 116. Interestingly, the Office of Legal Counsel at the U.S. Department of Justice has, at times, argued that the War Powers Resolution is constitutional. *Presidential Power to Use the Armed Forces Abroad Without Statutory Authorization*, 4A Op. Off. Legal Counsel 185 (1980) ("We believe that Congress may, as a general constitutional matter, place a 60-day limit on the use of our armed forces as required by . . . the Resolution . . . . We cannot say that placing that burden on the President unconstitutionally intrudes upon his executive powers.").

151 Carter, *supra* note 116, at 111 ("[The] evidence concerning the original understanding [of whether the War Powers Resolution would violate the executive's commander-in-chief function]—if one indeed chooses to put any faith in that means of constitutional adjudication—does not come down firmly on one side or the other.").

152 *Id.* at 129–33.

153 *See generally* MICHAEL JOHN GARCIA, CONG. RESEARCH SERV., RL30352, WAR POWERS LITIGATION INITIATED BY MEMBERS OF CONGRESS SINCE THE ENACTMENT OF THE WAR POWERS RESOLUTION (2012) (providing a case-by-case overview of the different actions taken by Congress members to force the President to abide by the War Powers Resolution).

154 *Id.* at 1.

155 *See, e.g.*, ABRAHAM D. SOFAER, WAR, FOREIGN AFFAIRS, AND CONSTITUTIONAL POWER (1976); Raoul Berger, *War-Making by the President*, 121 U. PA. L. REV. 29 (1972); Thomas F. Eagleton, *The August 15 Compromise and the War Powers of Congress*, 18 ST. LOUIS U. L.J. 1 (1973).

156 *See, e.g.*, Eugene V. Rostow, *Great Cases Make Bad Law: The War Powers Act*, 50 TEX. L. REV. 833 (1972) [hereinafter Rostow, *Great Cases Make Bad Law*]; J. Terry Emerson, *The War Powers Resolution Tested: The President's Independent Defense Power*, 51 NOTRE DAME L. REV. 187 (1975).

157 G. Sidney Buchanan, *In Defense of The War Powers Resolution:* Chadha *Does Not Apply*, 22 HOUS. L. REV. 1155, 1155 n.4 (1985) (suggesting that a legislative veto is "a provision by

Chadha decision is generally believed to have struck down section 5(c) of the War Powers Resolution, which permits the Congress to direct the President to remove the armed from a hostile situation by passage of a concurrent resolution."[158] In addition, some argue that Section 5(b) (requiring the removal of troops after the mandatory sixty-day period without congressional action, i.e., if only one chamber of Congress does not act) also represents a legislative veto.[159] In *Chadha*, the Supreme Court ruled that § 244(c)(2) of the Immigration and Nationality Act, which allowed Congress to pass a joint resolution forcing the Attorney General to cancel a deportation, was unconstitutional because it was a legislative veto of executive action.[160] Basing its decision on Article I, Section 7, Clauses 2 and 3 of the Constitution, the Supreme Court concluded that congressional action meant to have the effect of law must be approved by both houses of Congress and presented to the President for his approval (or disapproval).[161] In *Chadha*, "the Court held that § 244(c)(2) [was] unconstitutional because it authorized one house of Congress to change the legal status quo by action less than that required by the Constitution for a valid law."[162] As noted by Professor Sidney Buchanan however, substantial distinctions exist between § 244(c)(2) and the War Powers Resolution. For example, § 244(c)(2) allowed Congress to change the legal status quo by adjusting the legal status of the immigrant.[163] If, as some scholars argue, the War Powers Resolution is a codification of legally existing congressional war-making authority, then the War Powers Resolution does not change the legal status quo but merely fleshes out these powers.[164] Further, though scholars note that the War Powers Resolution may be unconstitutional because the action (of forcing the removal of troops) is not presented to the President for his approval, such presentment may not be required.[165] In *Hollingsworth v. Virginia*, the Supreme Court suggested that the presentment requirement applies only to

---

which Congress reserves to itself a power to affect, by later action less than a law, authority that it has previously delegated to some other agency or branch of government, typically to the executive branch or to an administrative agency exercising quasi-legislative, rule-making authority").

158 Daniel E. Lungren & Mark L. Krotoski, *The War Powers Resolution After the* Chadha *Decision*, 17 LOY. L.A. L. REV. 767, 777 (1984).

159 *Id.* at 782–93.

160 Immigration & Naturalization Serv. v. Chadha, 462 U.S. 919, 944–59 (1983). For a discussion of the facts of *Chadha* and the lower courts' decisions, see Buchanan, *supra* note 157, at 1170–73.

161 *Chadha*, 462 U.S. at 946–48.

162 Buchanan, *supra* note 157, at 1174.

163 *Id.* at 1177. For a discussion of other distinctions, see *id.* at 1177–79.

164 *Id.*

165 Carter, *supra* note 116, at 130.

"ordinary" cases of legislation.[166] This assertion implies that there may exist cases where legislation does not require presentment before the President and it is likely that a concurrent resolution in the War Powers Resolution would be extraordinary enough to fall into such a category.[167] As a result, it is unclear whether the War Powers Resolution represents an impermissible legislative veto.

Third, courts have suggested that members of Congress may have standing to bring suit based on violations of the War Powers Resolution.[168] Federal courts have suggested that, if Congress were to pass a resolution requiring a particular presidential report under the War Powers Resolution, for example, non-compliance with this resolution would constitute a cognizable claim.[169] As a result, Congress could potentially use the courts to bring a successful claim for violation of the War Powers Resolution.

Fourth and finally, some federal courts have asserted that the issue of whether the President refuses to abide by the War Powers Resolution is a political, non-justiciable question, and therefore the courts cannot rule on the matter.[170] At the same time, however, courts have also asserted that if a majority of Congress agreed that the President must abide by the requirements of the War Powers Resolution in a given circumstance, such consensus would present a justiciable claim to the courts.[171]

As this discussion illustrates, the War Powers Resolution is certainly flawed. However, it is not necessarily unconstitutional and may serve some

---

166 Hollingsworth v. Virginia, 3 U.S. 378, 381 n.* (1798) ("The negative of the President applies only to the ordinary cases of legislation: He has nothing to do with the proposition, or adoption, of amendments to the Constitution.").

167 For this argument, see Carter, *supra* note 116, at 130–33.

168 Dellums v. Bush, 752 F. Supp. 1141, 1147–48 (D.D.C. 1990); Crockett v. Reagan, 558 F. Supp. 893, 899 (D.D.C. 1982), *aff'd per curiam*, 720 F.2d 1355, 1357 (D.C. Cir. 1983) ("[W]ere Congress to pass a resolution to the effect that a report was required under the WPR, or to the effect that the forces should be withdrawn, and the President disregarded it, a constitutional impasse appropriate for judicial resolution would be presented.").

169 *Crockett*, 558 F. Supp. at 899; *see also* Lowry v. Reagan, 676 F. Supp. 333, 339 (D.D.C. 1987), *aff'd*, No. 87-5426 (D.C. Cir. 1988) (suggesting that if Congress enacted legislation to enforce the Resolution and the President ignored it, "a question ripe for judicial review" would be presented); *see also* GARCIA, *supra* note 153.

170 Sanchez-Espinoza v. Reagan, 568 F. Supp. 596, 601 (D.D.C. 1983), *aff'd*, 770 F.2d 202 (D.C. Cir. 1985) (declining to rule on whether the Reagan administration's actions triggered the War Powers Resolution because it presented a "nonjusticiable political question"); *see also* Conyers v. Reagan, 578 F. Supp. 324 (D.D.C. 1984), *aff'd*, 765 F.2d 1124 (D.C. Cir. 1985) (asserting that War Powers Resolution enforcement was a political, not a judicial, question). *But see* Campbell v. Clinton, 52 F. Supp. 2d 34, 40 n.5 (D.D.C. 1999), *aff'd*, 203 F.2d 19 (D.C. Cir. 2000) (suggesting that not every violation of the statute constituted a political question).

171 *Dellums*, 752 F. Supp. at 1150–51 (holding that an injunction could be issued and the President could be made to comply with the War Powers Resolution if there were congressional consensus on the issue).

positive function by alerting Congress to activities undertaken by the President and giving them the potential opportunity to weigh in, albeit not likely force the removal of U.S. forces. Thus, it still may prove useful in helping Congress regulate the use of offensive cyber operations, if it applies to them.

C. The War Powers Resolution as Applied to Offensive Cyber Operations

As discussed above, critical to the application of the War Powers Resolution—especially in the context of an offensive cyber operation—are the definitions of key terms, particularly "armed forces," as the relevant provisions of the Act are only triggered if the President "introduc[es armed forces] into hostilities or into situations [of] imminent . . . hostilities,"[172] or if such forces are introduced "into the territory, airspace, or waters of a foreign nation, while equipped for combat, except for deployments which relate solely to supply, replacement, repair, or training of such forces."[173] The requirements may also be triggered if the United States deploys armed forces "in numbers which substantially enlarge United States Armed Forces equipped for combat already located in a foreign nation."[174] As is evident, the definition of "armed forces" is crucial to deciphering whether the WPR applies in a particular circumstance to provide congressional leverage over executive actions. The definition of "hostilities," which has garnered the majority of scholarly and political attention,[175] particularly in the recent Libyan conflict,[176] will be dealt with secondarily here because it only becomes important if "armed forces" exist in the situation.

As is evident from a textual analysis,[177] an examination of the legislative history,[178] and the broad policy purposes behind the creation of the Act,[179]

---

172 50 U.S.C. § 1543 (2006).

173 *Id.*

174 *Id.*

175 *See, e.g.*, *War Powers: A Test of Compliance Relative to the Danang Sealift, the Evacuation of Phnom Penh, the Evacuation of Saigon, and the Mayaguez Incident: Hearings Before the Subcomm. on Int'l Sec. and Scientific Affairs of the H. Comm. on Int'l Relations*, 94th Cong. 38–39 (1975) (letter from State Dep't Legal Adviser Monroe Leigh & Dep't of Def. Gen. Counsel Martin R. Hoffmann to Chairman Clement J. Zablocki) [hereinafter Leigh & Hoffman] (defining "hostilities" "to mean a situation in which units of the U.S. armed forces are actively engaged in exchanges of fire with opposing units of hostile forces . . . .").

176 *Libya War Powers*, *supra* note 14, at 7–8.

177 Green v. Bock Laundry Mach. Co., 490 U.S. 504, 528 (1989) (Scalia, J., concurring) ("The meaning of terms on the statute books ought to be determined . . . on the basis of which meaning is [] most in accord with context and ordinary usage . . . .").

178 United Steelworkers of Am., AFL-CIO-CLC v. Weber, 443 U.S. 193, 226–44 (1979) (Rehnquist, J., dissenting) (illustrating how judges examine legislative history when interpreting statutes).

"armed forces" refers to U.S. soldiers and members of the armed forces, *not* weapon systems or capabilities such as offensive cyber weapons. Section 1547 does not specifically define "armed forces," but it states that "the term 'introduction of United States Armed Forces' includes the assignment of members of such armed forces to command, coordinate, participate in the movement of, or accompany the regular or irregular military forces of any foreign country or government."[180] While this definition pertains to the broader phrase "introduction of armed forces," the clear implication is that only *members* of the armed forces count for the purposes of the definition under the WPR. Though not dispositive, the term "member" connotes a human individual who is part of an organization.[181] Thus, it appears that the term "armed forces" means human members of the United States armed forces. However, there exist two potential complications with this reading. First, the language of the statute states that "the term 'introduction of United States Armed Forces' *includes* the assignment of members of such armed forces."[182] By using inclusionary—as opposed to exclusionary—language, one might argue that the term "armed forces" could include more than members. This argument is unconvincing however, given that a core principle of statutory interpretation, *expressio unius*, suggests that expression of one thing (i.e., members) implies the exclusion of others (such as non-members constituting armed forces).[183] Second, the term "member" does not explicitly reference "humans," and so could arguably refer to individual units and beings that are part of a larger whole (e.g., wolves can be members of a pack). As a result, though a textual analysis suggests that "armed forces" refers to human members of the armed forces, such a conclusion is not determinative.

An examination of the legislative history also suggests that Congress clearly conceptualized "armed forces" as human members of the armed forces. For example, disputes over the term "armed forces" revolved around *who* could be considered members of the armed forces, not *what* constituted a member. Senator Thomas Eagleton, one of the Resolution's architects, proposed an amendment during the process providing that the Resolution cover military officers on loan to a civilian agency (such as the Central

---

179 Church of the Holy Trinity v. United States, 143 U.S. 457, 459 (1892) ("It is a familiar rule, that a thing may be within the letter of the statute and yet not within the statute, because not within its spirit, nor within the intention of its makers.").

180 50 U.S.C. § 1547 (2006).

181 *See, e.g.*, *Member*, DICTIONARY.COM, http://dictionary.reference.com/browse/member?s=ts (last visited Oct. 22, 2012) (defining a "member" as a "person . . . that is part of a society, party, community, taxon, or other body").

182 50 U.S.C. § 1547 (2006) (emphasis added).

183 *See, e.g.*, TRW Inc. v. Andrews, 534 U.S. 19, 28–29 (2001).

Intelligence Agency).[184] This amendment was dropped after encountering pushback,[185] but the debate revolved around whether those military individuals on loan to the civilian agency were still members of the armed forces for the purposes of the WPR, suggesting that Congress considered the term to apply only to soldiers in the armed forces. Further, during the congressional hearings, the question of deployment of "armed forces" centered primarily on past U.S. deployment of troops to combat zones,[186] suggesting that Congress conceptualized "armed forces" to mean U.S. combat troops.

The broad purpose of the Resolution aimed to prevent the large-scale but unauthorized deployments of U.S. troops into hostilities.[187] While examining the broad purpose of a legislative act is increasingly relied upon only after examining the text and legislative history, here it provides further support for those two alternate interpretive sources.[188] As one scholar has noted, "[t]he War Powers Resolution, for example, is concerned with sending U.S. troops into harm's way."[189] The historical context of the War Powers Resolution is also important in determining its broad purpose; as the resolutions submitted during the Vietnam War and in the lead-up to the passage of the WPR suggest, Congress was concerned about its ability to effectively regulate the President's deployments of large numbers of U.S. troops to Southeast Asia,[190] as well as prevent the President from authorizing troop incursions into countries in that region.[191] The WPR was a reaction to the President's continued deployments of these troops into combat zones, and as such suggests that Congress's broad purpose was to prevent the unconstrained deployment of U.S. personnel, not weapons, into hostilities.

This analysis suggests that, when defining the term "armed forces," Congress meant members of the armed forces who would be placed in

---

184 Spong Jr., *The War Powers Resolution Revisited*, *supra* note 124, at 831.

185 *Id.*

186 *Congress, the President, and the War Powers: Hearings Before the Subcomm. on Nat'l Sec. Policy and Scientific Developments of the H. Comm. on Foreign Affairs*, 91st Cong. 124–31 (1970) [hereinafter *Congress, the President, and the War Powers*] (statement of John Norton Moore, Professor of Law, the University of Virginia School of Law).

187 50 U.S.C. § 1541 (2006).

188 YULE KIM, CONG. RESEARCH SERV., 97-589, STATUTORY INTERPRETATION: GENERAL PRINCIPALS AND RECENT TRENDS, CONG. RES. SERV. 2 (2008) ("[T]he Court has begun to place more emphasis on statutory text and less emphasis on legislative history and other sources 'extrinsic' to that text. More often than before, statutory text is the ending point as well as the starting point for interpretation.").

189 Dycus, *supra* note 76, at 162.

190 *See, e.g.*, Ratner & Cole, *supra* note 122, at 736.

191 *Congress, the President, and the War Powers*, *supra* note 186, at 124–31, 124 (statement of John Norton Moore, Professor of Law, the University of Virginia School of Law) (discussing congressional proposals to define the authority of the President to intervene abroad without congressional consent).

harm's way (i.e., into hostilities or imminent hostilities). Applied to offensive cyber operations, such a definition leads to the conclusion that the War Powers Resolution likely does not cover such activities. Worms, viruses, and kill switches are clearly not U.S. troops. Therefore, the key question regarding whether the WPR can govern cyber operations is not whether the operation is conducted independently or as part of a kinetic military operation. Rather, the key question is the delivery mechanism. For example, if military forces were deployed to launch the cyberattack, such an activity, if it were related to imminent hostilities with a foreign country, could trigger the WPR. This seems unlikely, however, for two reasons. First, it is unclear whether small-scale deployments where the soldiers are not participating or under threat of harm constitute the introduction of armed forces into hostilities under the War Powers Resolution.[192] Thus, individual operators deployed to plant viruses in particular enemy systems may not constitute armed forces introduced into hostilities or imminent hostilities. Second, such a tactical approach seems unlikely. If the target system is remote access, the military can attack it without placing personnel in harm's way.[193] If it is close access, there exist many other effective ways to target such systems.[194] As a result, unless U.S. troops are introduced into hostilities or imminent hostilities while deploying offensive cyber capabilities—which is highly unlikely—such operations will not trigger the War Powers Resolution.

IV. THE INTELLIGENCE AUTHORIZATION ACT: COVERT ACTIONS AND THE TRADITIONAL MILITARY ACTIVITIES EXEMPTION

Stemming from similar tension noted in the constitutional division of war-making authority noted above, congressional oversight of covert actions beyond intelligence collection has often proved a point of contention between the executive and legislative branches.[195] Presidents have "inferred authority [to conduct covert actions] from such places as the Vesting Clause, the Commander-in-Chief Clause, the Treaty Clause, and from an implied executive privilege."[196]

---

192 127 CONG. REC. 3743 (1981) (asserting that the hostility requirement is not triggered if personnel "will not act as combat advisors, and will not accompany . . . forces in combat, on operational patrols, or in any other situation where combat is likely"); *see also* Leigh & Hoffman, *supra* note 175 at 38–40.

193 *See* notes 87–98 and accompanying text.

194 *See* notes 87–89 and accompanying text.

195 *See generally* A. John Radsan, *An Overt Turn on Covert Action*, 53 ST. LOUIS UNIV. L.J. 485, 517–37 (2009) (detailing the development since 1947 of the congressional legal actions meant to limit executive covert actions).

196 *Id.* at 517.

Likewise, Congress attempted to rein in the President's ability to conduct covert operations without oversight by implementing a series of laws that required the President to get approval before undertaking such activities.[197] If the President did not provide such notification, Congress could decline to fund that particular covert activity.[198] Following the revelation that widespread, unreported covert actions were undertaken during the Vietnam War, Congress moved for stricter control of executive power, both by forcing the executive to account for the money it was spending as part of annual authorization bills[199] and by streamlining its own oversight capability by tasking two primary committees, the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, with oversight.[200]

While Congress designed this legislation to rein in the President's power to conduct covert activities without oversight, events in the 1980s clearly showed that its efforts had been ineffective.[201] In particular, the Iran-Contra affair illustrated that Congress needed to substantially reform oversight legislation to ensure that it could properly monitor executive covert action.[202] As a result, in 1990, Congress began drafting a new oversight bill,

---

197 Foreign Assistance Act of 1974 (Hughes-Ryan Act), Pub. L. No. 93-559, § 32, § 662, 88 Stat. 1795, 1804 (1974) (codified as amended at 22 U.S.C. § 2422 (1976)), *repealed by* Intelligence Authorization Act, Fiscal Year 1991, Pub. L. No. 102-88, 105 Stat. 429. The Hughes-Ryan Act, as amended, provided:

> No funds appropriated under the authority of this chapter or any other Act may be expended by or on behalf of the Central Intelligence Agency for operations in foreign countries, other than activities intended solely for obtaining necessary intelligence, unless and until the President finds that each such operation is important to the national security of the United States and reports, in a timely fashion, a description and scope of such operation to the appropriate committees of the Congress, including the Committee on Foreign Relations of the United States Senate and the Committee on International Relations of the United States House of Representatives.

Id.

198 Rasdan, *supra* note 195, at 522. ("Congress, by receiving notice of covert actions, could try to block an action it deemed inappropriate by denying funds to carry out the action.").

199 Marshall Silverberg, *The Separation of Powers and Control of the CIA's Covert Operations*, 68 TEX L. REV. 575, 596 (1990) ("This Act for the first time placed the CIA and the other intelligence agencies under congressional authorization and appropriation procedures.").

200 Intelligence Authorization Act for Fiscal Year 1981, Pub. L. No. 96-450, § 407(a), § 407(b)(1), § 501(a)(1), 94 Stat. 1975, 1981 (1980) (codified as amended at 50 U.S.C. § 413 (2000)); *see also* Rasdan, *supra* note 195, at 525–27.

201 Indeed, Congress itself remarked, in legislation meant to remedy its oversight failures associated with Iran-Contra, that "[u]nder current law . . . the Congressional mandate is ambiguous, confusing and incomplete. . . . The statutory requirements for informing the intelligence committees of covert actions are subject to misinterpretation, and the scope of activities covered by the law is undefined." S. REP. NO. 102-85, § 503, at 34 (1991).

202 *See generally* Report of the Congressional Committees Investigating the Iran Contra Affair, S. REP. NO. 100-216 (1987), H.R. REP. NO. 100-433 (1987) (detailing the Iran-Contra

the Intelligence Authorization Act of 1991, which grants Congress oversight of covert activities.[203] Section 413b of the Intelligence Authorization Act provides,

> To the extent consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters, the Director of Central Intelligence and the heads of all departments, agencies, and entities of the United States Government involved in a covert action . . . shall keep the [congressional] intelligence committees fully and currently informed of all covert actions . . . .[204]

The Act further provides that the President must ensure that any covert action that falls under the scope of the Act is reported to Congress "as soon as possible after such approval and before the initiation of the covert action"[205] unless "the President determines that it is essential to limit access to the finding to meet extraordinary circumstances affecting vital interests of the United States."[206] Moreover, if the President does not fully inform the intelligence committees *prior* to the action, he or she "shall fully inform the [congressional] intelligence committees in a timely fashion and shall provide a statement of the reasons for not giving prior notice."[207]

Congress, recognizing that the power of the statute turned—to a substantial degree—on the definition of covert action, provided guidance both in the legislation and the committee reports as to what the term meant. According to the statute, "the term 'covert action' means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly."[208] Congress also provided a list of exceptions to the term, however, specifically noting that, inter alia, "activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities,

---

scandal and resulting investigation); Harold Hongju Koh, *Why the President (Almost) Always Wins in Foreign Affairs: Lessons of the Iran-Contra Affair*, 97 YALE L.J. 1255 (1988) [hereinafter Koh, *Why the President (Almost) Always Wins in Foreign Affairs*] (arguing that the Iran-Contra Affair was symbolic of the inadequacies of America's foreign affairs policies).

203 50 U.S.C. §§ 413b(c)(2), 413b(d) (2006).

204 50 U.S.C. § 413b(b) (2006).

205 50 U.S.C. § 413b(c) (2006).

206 *Id.*

207 *Id.* Interestingly, President George H.W. Bush, when signing the bill, suggested that "timely fashion" did not mean within forty-eight hours, as specified in the Act. Rather, he suggested that "[i]n those rare instances where prior notice is not provided, I anticipate that notice will be provided within a few days. Any withholding beyond this period would be based upon my assertion of the authorities granted this office by the Constitution." Presidential Statement on Signing the Intelligence Authorization Act, Fiscal Year 1990, 2 PUB. PAPERS 1609, 1611 (Nov. 30, 1989).

208 50 U.S.C. § 413b(e) (2006).

traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities," as well as "traditional diplomatic or military activities or routine support to such activities," do not constitute covert action.[209]

While an initial textual reading of these exceptions—especially traditional military activities ("TMAs")—suggests that they are extremely broad, an examination of the Act's legislative history suggests that they are narrower than they first appear. In particular, as University of Texas law professor Robert Chesney notes, the Senate Select Committee on Intelligence's ("SSCI") committee report associated with the legislation,

> went on to make clear that the SSCI assumed that U.S. government responsibility 'would be apparent or acknowledged at the time of the military operation.' When that was not the case—i.e. when "military elements *not* identifiable to the United States [are] used to carry out an operation abroad without ever being acknowledged by the United States"—the operation would *not* constitute TMA.[210]

This original understanding led to an odd result, whereby "the TMA exemption did no work, as the definition of covert action already excluded operations in which the U.S. role was intended to be acknowledged."[211] To remedy this issue, the committees proposed, and President Bush ultimately accepted,[212] a compromise whereby an unacknowledged operation could fall under the traditional military activities exemption by meeting two requirements:[213] first, the TMA must be commanded and executed by military personnel; and second, the TMA must take place in a context in which overt hostilities are either ongoing or anticipated, meaning approval has been given by the National Command Authority (which consists of the President and the Secretary of Defense) for the activities and for the operational planning for hostilities.[214] Further, according to Chesney, "[o]perational planning can and normally will begin far earlier than the eve of conflict or even the eve of a deployment in anticipation of combat. . . . [T]he 'operational planning' standard . . . is not nearly as restrictive . . . as the casual reader might assume."[215]

---

209 *Id.*
210 Chesney, *supra* note 76, at 595.
211 *Id.* at 595–96.
212 *Id.* at 600–01.
213 *Id.* at 598–99.
214 S. REP. NO. 102-85, at 46 (1991).
215 Chesney, *supra* note 76, at 599–600.

A. The Intelligence Authorization Act as Applied to Offensive Cyber Operations

Given the language of the statute and the elaboration on its language provided by the legislative history, would offensive cyber operations—either used independently or in conjunction with a military campaign—trigger the notification requirements of the Intelligence Authorization Act? Looking first at cyber operations used prior to—or in conjunction with—military campaigns, the President would *not* need to report these to Congress under § 413b. Interestingly, depending on how the United States decides to conduct its offensive cyber operations, they may not even constitute covert actions under 413b, before even reaching the question of whether they fall under the exemptions. The statute's definition of covert actions requires that the United States not intend its role be "apparent or acknowledged publicly."[216] If, for example, the United States were to launch an attack using proxy forces—similar to the alleged Russian attack against Georgia in the 2008 war—it would likely constitute a covert action because the United States would be attempting to hide its role. Conversely, in the Israeli case, Israel likely did not intend for its computer attack against Syrian air defenses to remain hidden; indeed, by the overall attack's public nature, it seemed likely that information about the cyberattack preceding the military strike would be revealed. Likewise, if the United States in the lead-up to the Libya intervention had launched a cyberattack against the Libyan air defense network, it might also have failed to constitute covert action because of the likelihood that the third party observers would understand that a cyberattack occurred. Further, in the Israeli case and the Libya hypothetical, Israel and the United States clearly did not intend to hide their roles, as they followed the cyberattacks (or considered attacks) by openly striking targets within those countries.

If the United States did intend to hide a cyberattack, even though it was part of a larger military operation, such an attack would likely fall into the "traditional diplomatic or military activities or routine support to such activities" exception provided in the statute.[217] To qualify as a traditional military activity, the TMA must be commanded and executed by military personnel and take place in a context in which overt hostilities are either ongoing or anticipated, meaning approval has been given by the National Command Authority for the activities and for the operational planning for hostilities.[218] Given that the National Security Agency, responsible for the development and deployment of U.S. cyber capabilities, is co-housed and

---

216 50 U.S.C. § 413b(e) (2000).

217 *Id.*

218 S. REP. NO. 102-85, at 46 (1991).

extensively shares personnel with U.S. Cyber Command, the military command tasked with launching cyberattacks against adversaries, it seems likely that any such attack will satisfy the first prong of the test.[219]

Regarding the second prong, cyber operations conducted prior to, or in conjunction with, military operations may also take place in a context in which overt hostilities are either ongoing or anticipated. First, using the Russian activities in the 2008 war with Georgia as the basis for a factual hypothetical, if the United States were to conduct similar operations parallel to kinetic operations, such activity would be taking place in the context of overt hostilities. Though the level of hostilities is important in determining whether "overt hostilities" exist,[220] a Georgian-style conflict would likely trigger this exception.[221] Though one might argue, as the Obama administration did in the 2011 Libyan intervention, that its actions did not constitute hostilities (and therefore did not trigger the War Powers Resolution's reporting requirement), that argument does not hold force here because the Obama Administration was referring to the period *after* United States airmen were engaging in direct strikes against Libyan ground forces (and after all of Libya's air defenses were effectively destroyed).[222] By inference, the period in which U.S. forces were striking Libyan targets did constitute hostilities. Therefore, these cyber operations, used in conjunction with military operations, would likely fall under the TMA exception.

If the cyberattacks were used *prior* to the commencement of hostilities (for example if the United States launched OCOs to disable Libya's air defense network), they would also likely fall under the language of the exception because the National Command Authority would have given approval both for the activities and operational planning for the hostilities. While this might seem like a high burden, National Command Authority consists only of the President and the Secretary of Defense.[223] Thus the

---

219 Chesney, *supra* note 76, at 581 ("CYBERCOM and NSA are co-located at Fort Meade, they share some personnel (many of whom are trained in procedures meant to preserve a distinction between their actions as CYBERCOM personnel and their potentially-identical actions wearing their hats as NSA personnel), and both are (and must be) headed by the same official (currently General Keith Alexander).").

220 *See supra* notes 219–22 and accompanying text.

221 Roger N. McDermott, *Russia's Conventional Armed Forces and the Georgian War*, PARAMETERS, Spring 2009, at 65–67 (providing a short overview of the military elements of Russia's attack on Georgia).

222 *Libya War Powers*, *supra* note 14, at 7–9 ("The situation in Libya does not constitute a war requiring specific congressional approval under the Declaration of War Clause of the Constitution.").

223 Dep't of Def., Directive Number 5100.30, § 3.1 (Dec. 2, 1971) ("The NCA consists only of the President and the Secretary of Defense or their duly deputized alternates or successors.").

President and the Secretary of Defense must only approve the activities in anticipation of overt hostilities. Further, because operational planning can simply constitute planning for a "situation that likely would involve military forces in response to natural and man-made disasters, terrorists, subversives, military operations by foreign powers, or other situations as directed by the President or SecDef,"[224] National Command Authority for operational planning does not require the President and the Secretary of Defense to prepare to commence overt hostilities, but rather they can simply conduct contingency planning for a wide range of scenarios. Further, in a circumstance where the United States is prepared to actively intervene in another country, such as Libya, it would be clear that overt hostilities are anticipated, even in circumstances where overt hostilities are not imminent. In such a scenario, the President is merely considering future action and planning accordingly, and thus such offensive cyber operations would likely fall under the Traditional Military Activities exception.

Offensive cyber operations might also be exempt under the routine support exception. If the activity is "routine support" to "traditional diplomatic or military activities," it does not constitute covert action.[225] Though the legislation does not define "routine," the Senate committee suggested it involved a subjective element and that providing pertinent examples might be useful.[226] According to the committee, the term "would include various forms of logistical support that might be useful in placing personnel inside a denied area and enabling them to act without detection, including false documents, communications gear, safe houses, transportation, and information."[227] Interestingly, these examples seem to reference support to covert activities, not necessarily traditional military activities (i.e. helping to facilitate individuals to act without detection). However, if these activities are meant to support traditional military activities, then the language seems likely to encompass cyberattacks in preparation for military attacks against a target. For example, if the United States had launched OCOs against Libya to disable its air defense network in preparation of an allied air attack, this might be similar to aiding personnel in gaining access to a denied area (in this case, the personnel would be U.S. aircraft and the associated crewmen and the denied area would be airspace denied because of the defenses protecting it). While ambiguity certainly exists as to whether such a cyber operation would constitute routine support,

---

224 JOINT CHIEFS OF STAFF, *Joint Operational Planning*, JOINT PUBLICATION 5-0, Aug. 11, 2011, at xvii–xviii.

225 50 U.S.C. § 413b(e) (2006).

226 Chesney, *supra* note 76, at 596. *See also* S. REP. NO. 101-358, at 54 (1990) (providing examples of what the Committee would regard as "routine support").

227 Chesney, *supra* note 76, at 596.

offensive cyber operations conducted prior to—or in conjunction with—kinetic operations likely do fall under the covert action exemption.

Likewise, offensive cyber operations conducted independently of military operations, though likely constituting covert action, are also likely exempt under the Traditional Military Activities exception. Imagine, for example, that the United States launched the Stuxnet worm that attacked Iran's nuclear enrichment capabilities without Israeli involvement. Further imagine that all other facts in the case were the same as they are in reality (i.e. the United States denied its involvement in the attack). In such a case, the attack seems to constitute a covert action that requires reporting to the congressional intelligence committees because it was an activity to influence political conditions (i.e. the Iranian ability or decision to develop its nuclear program) or military conditions (i.e. preventing the Iranians from moving forward with the development of a nuclear weapon, which could substantially bolster their military capability) abroad.[228] Further, the United States did not intend for its role to be apparent or publicly acknowledged.[229]

Despite falling into this category, however, such an offensive operation, for the reasons discussed above, likely satisfies the congressional test for a traditional military activity. First, because General Alexander is the commander of both CYBERCOM and the head of the National Security Agency and because many of the personnel are dual-hatted at the respective organizations, any offensive cyber operation conducted independently of a kinetic assault will be commanded and executed by military personnel.[230] Second, because the President can launch offensive cyber operations without congressional notification if they are in anticipation of hostilities,[231] he also has great flexibility in deciding whether to report his activities. For example, if the President were to order the launch of a Stuxnet-style attack against Iran to degrade its nuclear enrichment capability, such an activity would—assuming it was done with the Secretary of Defense's consent—necessarily constitute approval by the National Command Authority. In addition, because the definition of operational planning—another element required in fulfilling the TMA exception to the definition of covert action—is so broad, such an attack would likely fall within its purview. The President would simply argue that approval has been given for operational planning of future combat operations with Iran (which it almost certainly has in the U.S. military)[232] and therefore the activity was taking place in the context where

228 50 U.S.C. § 413b(e) (2006).

229 *Id.*

230 S. REP. NO. 102-85, at 46 (1991).

231 *Id.*

232 *See, e.g.*, David E. Sanger & Annie Lowrey, *Iran Threatens to Block Oil Shipments, as U.S. Prepares Sanctions*, N.Y. TIMES (Dec. 27, 2011), www.nytimes.com/2011/12/28/world/

overt hostilities are anticipated. Indeed, only in a situation where no contingency planning has occurred—such as with an ally or a country that the United States takes little interest—would this exception *not* apply.

As a result, it becomes evident that even a Stuxnet-type of attack likely will not trigger the requirements set forth in the Intelligence Authorization Act. Given the dual-hatted nature of many NSA and CYBERCOM personnel, as well as the fact that action approved by the President and the Secretary of Defense necessarily constitutes approval by the National Command Authority, all the executive branch must realistically show is that it undertook the operation in a context where operational planning had occurred for potential hostilities at some undefined point in the future. This hurdle is very low and the executive should have little problem clearing it.

These limited requirements suggest that the executive can easily argue that offensive cyber operations conducted both as independent actions and in conjunction with kinetic operations likely fall under the Traditional Military Activity exception to the definition of covert action as provided by the Intelligence Authorization Act. As a result, the President is likely not statutorily required to report any offensive cyberattacks under the Act.

V. A MIDDLE GROUND OF LEGAL OVERSIGHT

This analysis suggests that, given inherent weaknesses in the underlying statutory schemes, excluding offensive cyber operations from their scope does not substantially shift the balance of war-making authority between the President and Congress. This exclusion does, however, provide the President additional, powerful means by which to conduct military action without congressional oversight.

Based on analysis of the War Powers Resolution, the lack of oversight for OCOs does not radically shift the balance between the legislative and executive branches' war-making authority. Most notably, because the War Powers Resolution itself has proven ineffective in providing Congress with a powerful tool to govern presidential use of force, bringing OCOs under the War Powers Resolution's statutory umbrella likely would not provide the possibility of such oversight. However, insofar as the President has increasingly turned to covert action since the passage of the War Powers Resolution to avoid its reporting requirements,[233] offensive cyber operations

middleeast/iran-threatens-to-block-oil-route-if-embargo-is-imposed.html ("In recent interviews, Obama administration officials have said that the United States has developed a plan to keep the strait[s] [of Hormuz] open in the event of a crisis.").

233 Koh, *Why the President (Almost) Always Wins in Foreign Affairs*, *supra* note 202, at 1273 (arguing that the WPR "only drove [executive war-making] underground, stimulating the

provide the President another means by which to continue this trend. OCOs therefore may give the President substantially more flexibility than he already has under the War Powers Resolution by adding what will become an increasingly frequent tool of warfare to his option-set.

The lack of congressional oversight of offensive cyber operations under the Intelligence Authorization Act also likely does not seriously shift the balance between congressional and executive war-making powers. The reason is inherent in the limitations of the legislation itself: the Intelligence Authorization Act specifies reporting requirements, but does not require the non-use or withdrawal of forces.[234] Further, these reports must be made in a "timely" fashion (the definition of which is undefined) and only to a small number of Congressmen (at most eight).[235] Thus even if the President had to report offensive cyber operations to Congress, it is unclear he would have to do so in a way that gave Congress an effective check, as these reports would be made only to a small group of Congressmen (who would not be able to share the information, because of its classified nature, with other members of the legislature) and could be done well after the employment of these capabilities. The resulting picture is one of increased presidential flexibility; the War Powers Resolution and the Intelligence Authorization Act—while arguably ineffective in many circumstances—provide increased congressional oversight of presidential war-making actions such as troop deployments and covert actions. Yet these statutes do not cover offensive cyber operations, giving the President an increasingly powerful foreign policy tool outside congressional reach.

Should these statutes be adjusted (or new ones created) that give Congress additional oversight in this area? Two competing desiderata suggest that oversight should be increased, but only to a limited extent. On the one hand, policymakers have suggested that developing strict rules and limitations on the use of offensive cyber operations will handicap the military's ability to quickly and effectively employ these tools in critical situations, such as cyber warfare against adversarial states.[236] According to these arguments, developing red lines that proscribe the use of these capabilities will create reluctance and trepidation among strategists and will lead to disadvantages in combat situations.[237] On the other hand, developing some legal rules is necessary to ensure that, as these cyber

---

Executive to substitute covert for overt operations and to transfer control of those operations from the military establishment to the intelligence agencies, particularly the CIA").

234 50 U.S.C. § 413b (2006).

235 Dycus, *supra* note 76, at 160.

236 Baker, *supra* note 24.

237 *Id.*

capabilities continue to develop, the President does not gain sufficient leverage to substantially tilt the balance between the President and Congress. Moreover, because these capabilities are still developing at a fast rate, understanding how they should and should not be employed is an important goal and having senior members of Congress and their staffs—professional staff members on the intelligence committees, who likely have substantial experience in these areas—provide input would be useful in developing this understanding.

These competing arguments—one for limiting any oversight and one for increasing it—suggest a middle ground that will avoid drawing red lines but will still provide useful congressional insight into the doctrinal and legal development of offensive cyber operations. Such an approach would include new legislation, similar to the Intelligence Authorization Act, explicitly requiring the President to report its use of covert cyber activities to the heads of Senate and House intelligence committees (i.e. the Gang of Eight).[238] Congress would not have the ability to veto such actions, however it would be able to raise potential legal issues with the executive branch, as well as provide policy advice as to the wisdom of employing these capabilities in such circumstances. As a result, while the heads of these committees would not have the ability to draw red lines themselves, they would be able to consult with the executive branch—as the branch employs these capabilities—to determine their likely legality and wisdom. While the President could ignore this advice, such an approach would at the very least keep Congress informed of the developing capabilities and their employment. With such an approach, Congress could play a meaningful role in the shifting and uncertain legal and policy realms of offensive cyber operations, which will undoubtedly become increasingly important as the United States and other nations develop and employ these capabilities with ever-greater frequency.

238 ALFRED CUMMING, CONG. RESEARCH SERV., R40691, SENSITIVE COVERT ACTION NOTIFICATIONS: OVERSIGHT OPTIONS FOR CONGRESS 1 (2011) (explaining that the "Gang of Eight" refers to leaders of the House and Senate and of their intelligence committees).